T.C.
SAKARYA UYGULAMALI BİLİMLER ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

KAOS TABANLI YENİ BİR ÇOKLU ORTAM ŞİFRELEME ARACININ GELİŞTİRİLMESİ

YÜKSEK LİSANS TEZİ

Tankut KURT

Enstitü Anabilim Dalı	**:**	**ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ**
Tez Danışmanı	**:**	**Doç. Dr. Metin VARAN**

Şubat 2020

T.C.
SAKARYA UYGULAMALI BİLİMLER ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

KAOS TABANLI YENİ BİR ÇOKLU ORTAM ŞİFRELEME ARACININ GELİŞTİRİLMESİ

YÜKSEK LİSANS TEZİ

Tankut KURT

Enstitü Anabilim Dalı : ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ

Bu tez 06.02.2020 tarihinde aşağıdaki jüri tarafından oybirliği / oyçokluğu ile kabul edilmiştir.

Prof. Dr. Yılmaz UYAROĞLU Jüri Başkanı	Doç. Dr. Metin VARAN Üye	Doç. Dr. Akif AKGÜL 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.

Tankut KURT

06.02.2020

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. Metin VARAN'a teşekkürlerimi sunarım.

Tez çalışması boyunca bilgi ve birikimini benimle paylaşan değerli meslektaşım Emre GÜLERYÜZ'e teşekkürü bir borç bilirim.

Hayatımın her aşamasında bana sonsuz destek olan sevgili aileme saygılarımı ve teşekkürlerimi sunarım.

İÇİNDEKİLER

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

BÖLÜM 1.
GİRİŞ ……. 1
1.1. Literatür ……. 2
1.2. Tezde Yapılan Çalışmalar ve Literatüre Katkısı …… 4

BÖLÜM 2.
KAOS …….……. 7
2.1. Kaotik Sistemler…….. 8
2.1.1. Ayrık zamanlı sistemler …….……..... 8
2.1.2. Sürekli zamanlı sistemler …….…… 9
2.2. Kaos Analizleri ……...…….……..... 10
2.2.1. Denge noktaları ve özdeğerler……..... 10
2.2.2. Faz portreleri…….…….. 11
2.2.3. Başlangıç şartlarına hassas duyarlılık analizi…….. 12
2.2.4. Lyapunov üstelleri …….……..... 13
2.2.5. Çatallaşma diyagramı ……..... 14

2.3. Referans Kaotik Sistemler……. 15
2.3.1. Lorenz sistemi……..... 17
2.3.2. Rössler sistemi…… 18
2.3.3. Chen sistemi…… 20
2.3.4. Rikitake sistemi …….. 21
2.3.5. Cai sistemi…….. 23
2.3.6. Sprott94b sistemi…… 24
2.3.7. Sundarapandian sistemi…….. 26
2.3.8. Zhou sistemi…….…….... 27
2.3.9. Lai4d sistemi……... 29
2.3.10. Hu5d sistemi……...…….. 30

BÖLÜM 3.

KRİPTOLOJİ ve RASTGELE SAYI ÜRETECİ……..……... 33
3.1. Kriptoloji ……....……... 33
3.1.1. Simetrik şifreleme ……..…… 34
3.1.2. Asimetrik şifreleme ……..……... 35
3.1.3. Kaos tabanlı şifreleme ……..……... 36
3.2. Rastgele Sayı Üreteci (RSÜ) ……..... 37
3.2.1. RSÜ çeşitleri……..……..…… 37
3.2.1.1. Sözde rastgele sayı üreteci (SRSÜ)…….. 37
3.2.1.2. Gerçek rastgele sayı üreteci (GRSÜ)……... 38
3.2.2. Rastgele sayı üreteçlerine uygulanan NIST testleri……..... 39
3.2.3. Kaos tabanlı RSÜ tasarımları ……..... 40
3.2.3.1. Mod alma yöntemi…….…….... 41
3.2.3.2. Desimalden ikilik tabana dönüştürme yöntemi……... 42
3.2.3.3. Kayan noktalı sayı yöntemi…….. 42
3.3. Güvenlik Analizleri ……... 44
3.3.1. Histogram analizi……..…….. 44
3.3.2. Korelasyon analizleri ve pearson korelasyon katsayıları.…… 44
3.3.3. Entropi analizi……..……..... 45

3.3.4. NPCR ve UACI analizleri……... 45
3.3.5. PSNR analizi……..…….…….……... 46
3.3.6. Harf frekans analizi……..……... 47

BÖLÜM 4.

ÇOKLU ORTAM VERİLERİ İÇİN KAOS TABANLI ŞİFRELEME ALGORİTMALARI ……..……..…….…….. 48

4.1. XOR Yöntemi…… 51
4.1.1. XOR yöntemi ile metin şifreleme ……... 52
4.1.2. XOR yöntemi ile görüntü şifreleme ……... 52
4.1.3. XOR yöntemi ile ses şifreleme…… 52
4.1.4. XOR yöntemi ile video şifreleme ……... 52
4.2. Tur Sayılı XOR Yöntemi……... 53
4.2.1. Tur sayılı XOR yöntemi ile metin şifreleme ……... 53
4.2.2. Tur sayılı XOR yöntemi ile görüntü şifreleme…… 54
4.2.3. Tur sayılı XOR yöntemi ile ses şifreleme…… 55
4.2.4. Tur sayılı XOR yöntemi ile video şifreleme ……... 55
4.3. S-kutusu & XOR Yöntemi……..... 56
4.3.1. S-kutusu & XOR yöntemi ile metin şifreleme …… 58
4.3.2. S-kutusu & XOR yöntemi ile görüntü şifreleme ……..... 58
4.3.3. S-kutusu & XOR yöntemi ile ses şifreleme …… 58
4.3.4. S-kutusu & XOR yöntemi ile video şifreleme …… 59
4.4. Tur Sayılı S-kutusu Yöntemi…….……. 59
4.4.1. Tur sayılı S-kutusu yöntemi ile metin şifreleme…….. 61
4.4.2. Tur sayılı S-kutusu yöntemi ile görüntü şifreleme…….. 61
4.4.3. Tur sayılı S-kutusu yöntemi ile ses şifreleme ……..... 62
4.4.4. Tur sayılı S-kutusu yöntemi ile video şifreleme ……..... 62

BÖLÜM 5.

KAOS TABANLI YENİ BİR ÇOKLU ORTAM ŞİFRELEME YAZILIM ARACI TASARIMI …….……..…… 63

5.1. Şifreleme ve Deşifreleme Panelleri……..……..... 64
5.2. Analiz Panelleri……..……..... 67

BÖLÜM 6.

KAOS TABANLI ÇOKLU ORTAM ŞİFRELEME ARACIYLA YAPILAN UYGULAMALAR ……..…….……... 71

6.1. Tur Sayılı XOR Yöntemi ile Metin Şifreleme ve Deşifreleme Uygulaması...……. 71
6.2. XOR Yöntemi ile Görüntü Şifreleme ve Deşifreleme Uygulaması…… 77
6.3. Tur Sayılı S-kutusu Yöntemi ile Ses Şifreleme ve Deşifreleme Uygulaması…….……..…….. 83
6.4. S-kutusu & XOR Yöntemi ile Video Şifreleme ve Deşifreleme Uygulaması…….……..…….. 88

BÖLÜM 7.

SONUÇ VE ÖNERİLER ……... 94

KAYNAKLAR ……... 97
ÖZGEÇMİŞ ……... 104

SİMGELER VE KISALTMALAR LİSTESİ

a	: Sistem parametresi
AES	: Gelişmiş Şifreleme Standardı
ASCII	: Bilgi değişimi için Amerikan standart kodlama sistemi
Avi	: Video dosyası formatı
b	: Sistem parametresi
c	: Sistem parametresi
C_{i}	: Görüntünün piksel değeri
dB	: Desibel
det	: Determinant
DES	: Veri Şifreleme Algoritması
docx	: Dosya formatı
d_t	: Faz değişkeninin değerleri arasındaki fark
dx	: Türev operatörü
FIPS	: Federal Bilgi İşleme Standartları
fps	: Saniyedeki kare sayısı
GRSÜ	: Gerçek rastgele sayı üreteci
GUI	: Grafiksel kullanıcı arayüzü
h	: Sistem parametresi
I	: Birim matris
IDEA	: Uluslararası Şifreleme Algoritması
IEEE	: Elektrik ve Elektronik Mühendisleri Enstitüsü
IEEE-754	: IEEE kayan noktalı sayı formatı
i	: İndis
j	: İndis
J	: Jakobiyen matrisi
$k1$	: Sistem parametresi

k2	: Sistem parametresi
L	: Görüntü için piksel değerlerinin toplam sayısı
m	: Bit dizisinde belirli sayıdaki bitlerden oluşan blok
M	: Görüntünün toplam satır sayısı
MATLAB	: Matrix Laboratory
ms	: Milisaniye
MSE	: Ortalama karesel hata
n	: Bit dizisi uzunluğu
N	: Görüntünün toplam sütun sayısı
NIST	: Ulusal Standartlar ve Teknoloji Enstitüsü
NPCR	: Net piksel değişim oranı
p	: Probability
PNG	: Görüntü dosyası formatı
PSNR	: Tepe sinyali gürültü oranı
r	: Pearson korelasyon katsayısı
R^m	: Reel sayılar kümesi
RC4	: Rivest Cipher
RK4	: 4. dereceden Runge-Kutta yöntemi
RK5	: 5. dereceden Runge-Kutta yöntemi
RGB	: Red, Green, Blue
RNG	: Random number generator
RSA	: Ronald, Shamir, Adleman
RSÜ	: Rastgele sayı üreteci
SHA	: Secure Hash Algorithm
SRSÜ	: Sözde rastgele sayı üreteci
t	: Zaman
t_0	: Başlangıç zamanı
txt	: Dosya formatı
u	: Durum değişkeni
u_0	: Durum değişkeninin başlangıç değeri
UACI	: Değiştirilen piksellerin ortalama değeri
v	: Durum değişkeni

v_0 : Durum değişkeninin başlangıç değeri

y : Durum değişkeni

y_0 : Durum değişkeninin başlangıç değeri

z : Durum değişkeni

z_0 : Durum değişkeninin başlangıç değeri

w : Durum değişkeni

w_0 : Durum değişkeninin başlangıç değeri

Wav : Ses dosyası formatı

x : Durum değişkeni

x_0 : Durum değişkeninin başlangıç değeri

$\vec{x}$: Durum vektörü

XOR : Özel veya

λ : Özdeğerler veya Lyapunov üsteli

β : Sistem parametresi

σ : Sistem parametresi

ρ : Sistem parametresi

μ : Sistem parametresi

ŞEKİLLER LİSTESİ

Şekil 2.1. Kaos durumları…. 7
Şekil 2.2. Henon çekicisine ait görüntü…… 9
Şekil 2.3. Lorenz sisteminin x-z faz portresi…… 10
Şekil 2.4. 3 boyutlu kaotik bir sistemin durum değişkenlerinin zamana göre değişimi…… 11
Şekil 2.5. Örnek kaotik sistemin 2 boyutlu faz portresi…… 12
Şekil 2.6. Örnek sistemin başlangıç şartlarına olan hassas duyarlılığını gösteren zaman serileri……... 13
Şekil 2.7. Örnek bir çatallaşma diyagramı……. 15
Şekil 2.8. Lorenz sisteminin faz değerleri - zaman grafiği……. 17
Şekil 2.9. Lorenz sistemi faz portreleri…….. 18
Şekil 2.10. Rössler sisteminin faz değerleri - zaman grafiği…….. 19
Şekil 2.11. Rössler sistemi faz portreleri…… 19
Şekil 2.12. Chen sisteminin faz değerleri - zaman grafiği…….. 20
Şekil 2.13. Chen sistemi faz portreleri……... 21
Şekil 2.14. Rikitake sisteminin faz değerleri - zaman grafiği…… 22
Şekil 2.15. Rikitake sistemi faz portreleri…….. 22
Şekil 2.16. Cai sisteminin faz değerleri - zaman grafiği……. 23
Şekil 2.17. Cai sistemi faz portreleri…….. 24
Şekil 2.18. Sprott94b sisteminin faz değerleri - zaman grafiği…… 25
Şekil 2.19. Sprott94b sistemi faz portreleri…… 25
Şekil 2.20. Sundarapandian sisteminin faz değerleri - zaman grafiği……. 26
Şekil 2.21. Sundarapandian sistemi faz portreleri…….. 27
Şekil 2.22. Zhou sisteminin faz değerleri - zaman grafiği…… 28
Şekil 2.23. Zhou sistemi faz portreleri……... 28
Şekil 2.24. Lai4d sisteminin faz değerleri - zaman grafiği……. 29

Şekil 2.25. Lai4d sistemi faz portreleri…….. 30
Şekil 2.26. Hu5d sistemi faz portreleri……... 31
Şekil 2.27. Hu5d sisteminin faz değerleri - zaman grafiği…… 32
Şekil 3.1. Simetrik şifreleme akış diyagramı……. 35
Şekil 3.2. Asimetrik şifreleme akış diyagramı…… 36
Şekil 3.3. Mod alma yöntemi akış diyagramı……. 41
Şekil 3.4. Desimalden ikilik tabana dönüştürme yöntemi akış diyagramı……. 42
Şekil 3.5. Kayan noktalı sayı yöntemi akış diyagramı……... 43
Şekil 3.6. Kayan noktalı sayı yöntemi örnek gösterimi…….. 43
Şekil 4.1. Bir görüntüdeki piksellerin gösterimi…… 49
Şekil 4.2. XOR yönteminin akış diyagramı……... 51
Şekil 4.3. Tur sayılı XOR yönteminin akış diyagramı…….. 53
Şekil 4.4. S-kutusu & XOR yönteminin akış diyagramı…… 57
Şekil 4.5. Tur sayılı S-kutusu yönteminin akış diyagramı……. 61
Şekil 5.1. Yazılım aracının açılış ekranı……. 63
Şekil 5.2. Yazılım aracının şifreleme paneli……. 65
Şekil 5.3. Textten al seçiminin yapılmasıyla oluşan "Şifreleme Yöntem Seçimi" ekranı…… 66
Şekil 5.4. Yazılım aracının metin şifreleme analiz paneli……. 68
Şekil 5.5. Yazılım aracının ses şifreleme analiz paneli……. 69
Şekil 5.6. Yazılım aracının görüntü & video şifreleme analiz paneli…… 70
Şekil 6.1. Tur sayılı XOR yöntemi ile metin şifreleme işlemi……. 73
Şekil 6.2. Tur sayılı XOR yöntemi ile metin şifreleme analiz sonuçları……... 74
Şekil 6.3. Tur sayılı XOR yöntemi ile metin deşifreleme işlemi……. 76
Şekil 6.4. XOR yöntemi ile görüntü şifreleme işlemi……... 78
Şekil 6.5. XOR yöntemi ile görüntü şifreleme analiz sonuçları……. 79
Şekil 6.6. XOR yöntemi ile görüntü şifreleme analizlerinin rapor çıktısı……... 80
Şekil 6.7. XOR yöntemi ile görüntü deşifreleme işlemi…… 81
Şekil 6.8. Tur sayılı S-kutusu yöntemi ile ses şifreleme işlemi……... 84
Şekil 6.9. Tur sayılı S-kutusu yöntemi ile ses şifreleme analiz sonuçları……... 85
Şekil 6.10. Uygulamada kullanılan kaotik sistemin x ve z fazından elde edilen rastgele sayılar…… 86

Şekil 6.11. Tur sayılı S-kutusu yöntemi ile ses deşifreleme işlemi.……...… 87
Şekil 6.12. Kaotik sistemlerde başlangıç şartlarının etkisini gösteren başarısız bir deşifreleme işlemi……..…… 88
Şekil 6.13. S-kutusu & XOR yöntemi ile video şifreleme işlemi……... 90
Şekil 6.14. S-kutusu & XOR yöntemi ile video şifreleme analiz sonuçları…… 91
Şekil 6.15. S-kutusu & XOR yöntemi ile video deşifreleme işlemi…….. 93

TABLOLAR LİSTESİ

Tablo 2.1. Lyapunov üstellerin işaretlerine göre durumları.…..……... 14
Tablo 4.1. Metin şifreleme uygulamaları için kullanılacak karakterlerin ASCII kod değerleri.…….. 49
Tablo 4.2. Örnek bir 16 x 16'lık S-kutusu……. 57
Tablo 6.1. Uygulamaların gerçekleştirildiği bilgisayarın özellikleri……..... 71
Tablo 6.2. Chen sisteminden üretilen değerlerin NIST 800-22 testi sonuçları….. 72
Tablo 6.3. Lorenz sisteminden üretilen değerlerin NIST 800-22 testi sonuçları... 77
Tablo 6.4. Görüntü şifreleme uygulamalarının analiz sonuçlarının karşılaştırılmaları…… 82
Tablo 6.5. Zhou sisteminden üretilen değerlerin NIST 800-22 testi sonuçları….. 83
Tablo 6.6. Cai sisteminden üretilen değerlerin NIST 800-22 testi sonuçları……. 89

KAOS TABANLI YENİ BİR ÇOKLU ORTAM ŞİFRELEME ARACININ GELİŞTİRİLMESİ

ÖZET

Günümüzde teknolojinin gelişmesiyle dijital ortamda güvenliliğin gerekliliklerini sağlayacak olan araçlara ihtiyacımız hızla artmıştır. Bu nedenle verilerin şifrelenmesi hususu önemli bir durum haline gelmiştir. Kriptoloji şifre bilimidir ve çeşitli verilerin belirli bir sisteme göre şifrelenmesi, deşifre edilmesi işlemlerini kapsamaktadır. Askeri, ticari ve tıbbi veri tabanları gibi gizli olması gereken alanların yanında bireysel bilgi güvenliğine olan yoğun talepler kriptoloji çalışmalarının önemini her geçen gün arttırmaktadır. Son yıllarda standart şifreleme yöntemlerinin yanı sıra kaos tabanlı şifreleme yöntemleri de kriptoloji bilim dalının kritik olarak kullanıldığı alanlarda yer almaya başlamıştır. Başlangıç şartlarına karşı hassas duyarlılık gösterme, periyodik olmama, geniş bir frekans bandında kullanılabilme ve zengin dinamik davranışlar göstermesi gibi özellikleri kaos tabanlı şifrelemenin kriptoloji uygulamalarında yaygın olarak kullanılabilme potansiyelini arttırmaktadır.

Bu çalışmada kaotik sistem tabanlı çalışan XOR, Tur sayılı XOR, S-kutusu & XOR ve Tur sayılı S-kutusu şifreleme yöntemleri önerilerek; metin, görüntü, ses ve video çoklu ortam verileri için bu yöntemler kullanılmak üzere şifreleme ve deşifre etme işlemleri uygulanmıştır. Önerilen tüm şifreleme algoritmaları, kaotik sistemlerin çıkış değerlerinin rastgele sayı üreteci olarak kullanılmasıyla gerçekleştirilmiştir. Rastgele sayıların elde edilmesi için 3 adet rastgele sayı üreteci tasarım çalışması önerilmiştir. Önerilen tasarım çalışmaları mod alma, desimalden ikilik tabana dönüştürme ve kayan noktalı sayı yöntemleridir.

Şifreleme yöntemlerinin kolay, doğru ve kullanışlı bir şekilde uygulanabilmesi için MATLAB® programında bir yazılım aracı tasarımı geliştirilmiştir. Şifreleme yöntemlerinde kullanılacak rastgele sayıların üretilebilmesi için literatürde bulunan bazı kaotik sistemler yazılım aracı içerisine eklenmiştir. Yazılım aracı, içerisinde mevcut olmayan kaotik sistemlerin de eklenmesiyle rastgele sayıların üretilebileceği veya şifrelemede direkt olarak kullanılacak olan rastgele sayıların aktarılabileceği bir fonksiyona sahiptir.

Şifreleme işlemleri için kaotik sistemlerden elde edilen sayıların NIST 800-22 testinden çıkan p (probability) sonuç değerlerinin istenen değerlerde olduğu belirlenmiş ve sayıların, rastgele sayılar olduğu kanıtlanmıştır. Yapılan şifreleme işlemleriyle elde edilen verilerin deşifre etme işlemleri sonucunda orijinal halleri yeniden elde edilmiştir. Şifreleme sonrası yazılım aracında yapılan bazı güvenlik analizleriyle de önerilen şifreleme yöntemlerinin gizlilik ve bilgi güvenliği gerektiren uygulamalarda kullanılmak üzere başarılı sonuçlar veren yöntemler olduğu gösterilmiştir.

Anahtar kelimeler: Kaos, Kaotik sistemler, Kriptoloji, RSÜ, MATLAB®, S-kutusu, XOR, Çoklu ortam, Güvenlik analizleri, NIST, Yazılım Aracı

DEVELOPMENT OF A NEW MULTIMEDIA ENCRYPTION TOOL BASED ON CHAOS

SUMMARY

At present, the need for tools to ensure security in the digital environment has shown a rapid increase with the development of technology. Because of this reason, data encryption has become an important position. Cryptology is the science of cipher, and it involves the process of encrypting and decrypting various data according to a specific system. Military, commercial and medical databases, as well as the need to be confidential areas of the individual information security demands on the importance of cryptology work is increasing every day. In recent years, chaos-based encryption methods, as well as standard encryption methods, have started to take place in areas where cryptology is used critically. Chaos-based encryption has different features such as non-periodicity, wide frequency band usage, generous dynamic behavior and showing the sensitivity against the initial conditions. These features increase the potential of chaos-based encryption to be widely used in cryptology applications.

In the thesis, XOR, Circuit XOR, S-box & XOR, and Circuit S-box encryption methods working based on the chaotic system are proposed; encryption and decryption processes were applied to use these methods for text, image, audio and video multimedia data. All proposed encryption algorithms are performed by using the output values of chaotic systems as random number generators. Random number generator design studies have been proposed to obtain random numbers. Proposed design studies include mod retrieval, conversion from desimal to binary base, and floating-point number methods.

A software tool has been developed in MATLAB® to make these encryption methods easy, accurate and convenient. So as to achieve generation random numbers to be used in encryption methods, some chaotic systems in the literature have been added to the software tool. The software tool has a function in which random numbers can be generated by adding chaotic systems -that are not present in the software tool- or to which random numbers can be transmitted directly to be used in encryption.

The numbers obtained from the chaotic systems for encryption operations, p (probability) result values from the NIST 800-22 test were determined to be the desired value and these numbers were proved to be random numbers. The data obtained with the encryption operations, as a result of the deciphered process, was recovered from the original state. It has been shown that the proposed encryption methods are successful methods to be used in applications requiring confidentiality and information security with some security analyzes performed in the post-encryption software tool.

Keywords: Chaos, Chaotic systems, Cryptology, RNG, MATLAB®, S-box, XOR, Multimedia, Security analyzes, NIST, Software tool

BÖLÜM 1. GİRİŞ

Kaos teorisi, belirli koşulların bulunduğu durumda kaos olarak bilinen bir fenomen sergileyen bazı doğrusal olmayan dinamik sistemlerin davranışını açıklar. Kaos kısa tabirle düzensizliğin düzeni ifadesiyle tanımlanabilir. Kaos koşullarının oluştuğu dinamik sistemler, kaotik sistemler olarak adlandırılır [1].

Kaotik sistemler, bir meteorolog ve matematikçi olan Edward Lorenz tarafından keşfedilmiştir. Lorenz, 1963 yılında meteorolog olarak çalışmalar gerçekleştirirken üç değişkenli bir sistemde başlangıç şartlarında oluşan çok küçük değişimlerin belirli bir süre sonunda öngörülemez sonuçlar doğurabileceğini göstermiştir [2]. Kaos kelimesi literatürde ilk kez T. Y. Li ve J. A. Yorke'nin 1975 yılında yayınlamış oldukları makalede kullanılmıştır [3].

Kaotik sistemlerin; sistemde bulunan parametreler ile başlangıç şartlarına hassas bağımlı olmaları, periyodik olmamaları ve zengin dinamik davranışlar göstermeleri başlıca özellikleri arasında sayılabilir [4]. Kaotik sistemler başlangıç durumundan sonraki iterasyonlarda oluşan yeni durumlar neticesinde rastgele davranıyormuş gibi önceden kestirilmesi mümkün olmayan durumlara geçmektedirler. Bu gibi özellikleri kaos teoreminin çeşitli alanlarda kullanılmasının önünü açmaktadır. Bu alanlara biyomedikal, mekatronik, biyoloji, fizik, haberleşme, robotik, bulanık mantık ve elektronik devreler gibi örnekler verilebilir [5-12]. Kriptoloji bilimi de kaos teorisiyle ilişkisi olan uygulama alanlarından birisidir.

Kriptoloji, haberleşme gizliliğinin sağlanabilmesi, verilerin saklanması ve korunması durumları hakkında çalışan bir bilim dalıdır. Kriptoloji, kriptografi ve kriptoanaliz olarak iki bölüme ayrılır. Kriptografi, verinin şifrelenmesi işlemidir. Çözümü çok zor olan matematik problemlerini ve sistemleri inceler. Kriptoanaliz de bu matematik problemlerini çözmeye çalışma veya şifreyi çözme işlemi olarak tanımlanabilir [13].

Bir haberleşme uygulamasında mesajı gönderen taraf gönderici, mesajın ulaştığı tarafsa alıcı olarak adlandırılır. Gönderici, gönderdiği verinin içeriğinin herhangi bir kişi tarafından görülmesini istemediğinden dolayı veriyi belirli bir sisteme göre değiştirme yani şifreleme yoluna başvurur. Alıcı da şifrelenmiş olan veriyi belirli bir sisteme göre çözüp orijinal haline getirmek için deşifre etme işlemini gerçekleştirir.

Tez çalışması kapsamında önerilen tüm şifreleme yöntemlerinde S-kutuları ve XOR işlem yapısının tekil veya çoğul olarak kullanımı uygulanmıştır. S-kutusu doğrusal olmayan bir yapıda olup şifreleme algoritmalarında karıştırma işlemi yapan dolayısıyla algoritmaya gücünü veren elemandır. İyi bir S-kutusu seçimi şifrelemenin karmaşık ve başarılı olmasını direkt olarak etkiler. S-kutularının bir kullanım şekli de sözde rastgele sayı üreteci olarak kullanılmalarıdır [14]. Bu çalışmada S-kutularının kullanıldığı yöntemlerde şifrelenecek veri, S-kutularında karşılığı bulunan değerlere göre bir değer değişimine uğramaktadır. XOR işleminin bulunduğu şifreleme yöntemlerinde ise rastgele sayılardan oluşan şifreleme anahtarı, şifrelenecek veriyle veya bir S-kutusu dönüşümüne uğramış veriyle XOR işlemine girmektedir.

Teknolojinin gelişmesiyle dijital ortamda güvenliliğin gerekliliklerini sağlayan araçlara olan ihtiyaç hızla artmaktadır. Bu nedenle verilerin şifrelenmesi hususu önemli bir durum haline gelmiştir Askeri, ticari ve tıbbi veri tabanları gibi gizliliğin olması gereken alanlarda kriptoloji bilim dalı yoğunlukla kullanılmaktadır. Verilere izinsiz erişim gibi olumsuz durumları ortadan kaldırmak için de kriptolojinin çalışma konusu olan bazı şifreleme yöntemleri geliştirilmiştir. Günümüzde şifreleme uygulamalarında sıkça kullanılmaya başlanan kaos teorisi ile halihazırda literatürde bulunan şifreleme yöntemlerine alternatif çalışmalar gerçekleştirilmeye başlanmıştır.

1.1. Literatür

Kaos teoremine dair ilk çalışmalar 1963 yılında Edward Lorenz tarafından hava değişimleri ile ilgili yapmış olduğu diferansiyel denklem çalışmaları ile başlamıştır. Lorenz, bulmuş olduğu denklemlerin hassas başlangıç değerlerine bağımlı olduğunu keşfetmiştir [2].

Haberleşme sistemlerinde kaos teorisi kullanılarak veriyi taşıma ve şifreleme düşüncesi, Pecora ve Carroll tarafından 1990 yılında iki adet farklı kaotik osilatörün

senkronizasyonun gerçekleşebileceğinin tespit edilmesiyle ortaya koyulmuştur [15]. Cuomo ve arkadaşları Lorenz kaotik sisteminin devre gerçekleştirmesini yapmış, güvenli bir haberleşme için kaotik maskeleme ve senkronizasyon hatalarının algılanması ilkesine dayanan iki değişik yaklaşımda bulunmuşlardır [16]. Matthews tarafından yapılan çalışmada bir kaotik şifreleme algoritması geliştirilmiştir. Metin verileri için gerçekleştirilen çalışmada, Lojistik Denklemde tam sayılı tekrarlamalar için bir metin mesajında mevcut olan her bir karakterin şifrelenmesine dayalı olan basit tek boyutlu denklemler geliştirilmiştir [17].

Wong ve arkadaşları, yapmış oldukları çalışmada kaotik Standart Map sistemini kullanarak basit ekleme ve değiştirme işlemlerine dayalı bir görüntü şifreleme çalışması gerçekleştirmişlerdir. Oluşturdukları kaos tabanlı şifreleme algoritmasını hızlandırmaya ve böylelikle şifreleme süresini minimize etmeye çalışmışlardır. Çalışmanın sonucunda gri tonlamalı 512 x 512 boyutlarında olan bir görüntüyü 100 ms'nin altında şifrelemeyi başarmışlardır [18]. Wang ve arkadaşları, yapmış oldukları kaos tabanlı görüntü şifreleme çalışmasında her adım için farklı kontrol parametreleri meydana getirerek güçlü bir algoritma elde etmeyi hedeflemişlerdir. Bu algoritma ile görüntü her adımda farklı bir anahtar ile şifreleme işlemine girmiş ve şifreleme işleminde hız ve güvenlik kriterleri açısından başarılı sonuçlara ulaşılmıştır [19].

Xiao ve arkadaşları, yaptıkları çalışmada Arnold Cat Map ve Chen kaotik sistemlerinden yararlanarak gri tonlamalı görüntü şifreleme algoritması geliştirmişlerdir. Yapmış oldukları çalışmanın sonucunda güvenlik testlerinden başarılı sonuçlar elde edildiği görülmektedir [20]. Hongjun ve Xingyuan, yapmış oldukları kaotik tabanlı görüntü şifreleme uygulamasında Chebyshev Map kaotik sisteminden yararlanarak görüntüde oluşan gürültülere karşı güçlendirilmiş bir algoritma geliştirmişlerdir. Oluşturdukları algoritmayla şifrelenmiş görüntüdeki gürültüye rağmen en az kayıpla orijinal görüntüye ulaşmışlardır [21].

Liu ve Wang, aynı boyutlarda olan üç farklı görüntünün sırasıyla kırmızı, yeşil ve mavi kanallarını birleştirerek şifreleme ve deşifreleme uygulaması gerçekleştirmişlerdir. Şifrelemede kullanılacak anahtar için SHA-256 hash fonksiyonundan ve rastgele sayı üreteci olarak Lorenz kaotik sisteminin faz çıkış değerlerinden yararlanmışlardır [22]. Prusty ve arkadaşları yaptıkları görüntü şifreleme çalışmasında Arnold Cat Map sistemini

kullanarak görüntüyü karıştırmış ve Henon Map sistemini kullanarak anahtar üretip değişik formatlardaki görüntü verilerini şifreleyerek başarılı sonuçlar elde etmişlerdir [23].

Alsafasfeh ve Arfoa, yapmış oldukları çalışmada Lorenz kaotik sistemini Rössler kaotik sistemine ekleyerek yeni bir kaotik sisteme dayanan bir şifreleme uygulaması ileri sürmüşlerdir. Yapmış oldukları analizler sonucunda bu yeni algoritmanın hız ve yüksek güvenlilik avantajlarına sahip olduğunu açıklamışlardır [24]. Fındık, yaptığı çalışmada kaos tabanlı olan ve kaos tabanlı olmayan şifreleme algoritmalarını karıştırarak metin şifreleme uygulaması gerçekleştirmiş ve gerçekleştirmiş olduğu uygulamaya dair başarılı sonuçlar almıştır [25]. Liu ve arkadaşları, renkli görüntülerin kaos tabanlı bir blok şifreleyici sistem ile şifrelenmesine yönelik çalışmalar gerçekleştirmişlerdir. Yapılan çalışmada histogram, korelasyon, diferansiyel atak ve entropi analizlerinin sonuçlarıyla başarılı bir şifreleme işleminin yapıldığı gösterilmiştir [26].

Ahmad ve arkadaşları, yaptıkları çalışmada ses verilerini şifrelemek için kaos tabanlı bir anahtar akış üreteci önermişlerdir. Yapılan çalışmanın deneysel analizleri sonucunda bu yöntemin ses verilerinin şifrelenmesinde yüksek güvenlilik sağladığı belirtilmiştir [27]. Abdulkareem ve Abduljaleel, yaptıkları çalışmada ses verilerini şifrelemek için tek boyutlu bir kaotik sistem ile Blowfish şifreleme metodunu kullanarak yeni bir şifreleme metodu geliştirmişlerdir [28]. Akgül tarafından yapılan çalışmada, yeni kaotik sistemler önerilerek rastgele sayı üreteci (RSÜ) tabanlı özgün bir algoritma ile çoklu ortam verilerinin şifreleme uygulamaları gerçekleştirilmiştir. Yapılan analizler sonucunda önerilen kaos tabanlı şifreleme yönteminin yüksek güvenlik seviyesinde olduğu gösterilmiştir [29].

1.2. Tezde Yapılan Çalışmalar ve Literatüre Katkısı

Bu tez çalışmasında kriptoloji biliminde sıkça kullanılan kaotik sistemlerden yararlanılarak kaos tabanlı yeni şifreleme algoritmaları ile programlanmış bir şifreleme yazılım aracının oluşturulması üzerine çalışılmıştır. Yazılım aracında 4 farklı şifreleme algoritması mevcuttur. Tüm şifreleme algoritmalarında çoklu ortam verileri anahtarlar aracılığıyla şifrelenir. Bu anahtarlar kaotik sistemlerin çıkış değerlerinden elde edilen

rastgele sayılarla oluşturulur. Rastgele sayıların elde edilmesi için 3 adet rastgele sayı üreteci tasarım çalışması yapılmıştır.

Tasarlanan yazılım aracında referans kaotik sistemlerin bulunmasının dışında yazılım aracı, içerisine kullanıcı tarafından alternatif kaotik sistemlerin eklenip Runge-Kutta 4 (RK4) sayısal analiz yöntemine göre çözdürülmesine ve sonrasında da bu sistemlerin kaydedilmesine imkân sağlamaktadır.

Yazılım aracı şifrelemede anahtar olarak kullanılacak rastgele sayıların nasıl seçilebileceği ile ilgili üç seçenek sunmaktadır. Bu seçimler; yazılım aracında bulunan mevcut kaotik sistemlerin değerlerinden üretilen rastgele sayılar, kullanıcı tarafından farklı kaotik sistemlerin yazılım aracına eklenmesiyle süregelen çözdürme işlemleriyle üretilen rastgele sayılar ve direkt olarak rastgele sayıların bulunduğu "*txt*" dosya girişi ile gerçekleştirilir. Şifrelenen verinin türüne göre şifreleme sonrası oluşturulan güvenlik analizlerinin tasarlanan yazılım aracı üzerinden yapılması suretiyle her uygulama sonrasında şifreleme kalitesi hakkında bilgilere ulaşılır. Yapılan bu güvenlik analizlerinin sonuçlarına kullanıcı tarafından daha kolay ulaşılabilmesi için yazılım aracına raporlama birimi entegrasyonu yapılmıştır.

Bu tez çalışmasında standart şifreleme türlerine alternatif olarak geliştirilen şifreleme yöntemleri ile daha güvenilir yapıda olan şifreleme algoritmalarının geliştirilmesi ve bu şifreleme algoritmalarının kolay, doğru ve kullanışlı bir şekilde uygulanabilmesi için bir yazılım aracı tasarımı geliştirilmesi amaçlanmıştır.

Bu amaçlar doğrultusunda tezin ikinci bölümünde kaos teorisi, kaotik sistemler, kaotik sistemler ile ilgili yapılan analizler hakkında bilgiler verilmiş ve yazılım aracı içerisinde kullanılan referans kaotik sistemler tanıtılmıştır.

Üçüncü bölümde, kriptoloji bilimi ve rastgele sayı üreteci kavramları açıklanmış, rastgele sayıların elde edilmesi için tasarlanan rastgele sayı üreteçlerinin (mod alma yöntemi, desimalden ikilik tabana dönüştürme yöntemi ve kayan noktalı sayı yöntemi) çalışma yapılarını gösteren diyagramlarla birlikte örnekler ortaya konmuş ve sayı dizilerinin rastgeleliğinin ölçümünde yararlanılan NIST 800-22 testinin özelliklerinden bahsedilmiştir. Ayrıca tez çalışması kapsamında yapılacak olan şifreleme uygulamalarının içerisinde bulunan güvenlik analizlerinin tanıtımı bu bölümde gerçekleştirilmiştir.

Dördüncü bölümde metin, görüntü, ses ve video çoklu ortam verilerinin sayısal değerlerinin elde edilişi ile ilgili açıklamalar yapılmış ve çoklu ortam verilerinin her biri için önerilen 4 şifreleme yöntemi (XOR, Tur sayılı Xor, S-kutusu & XOR, Tur sayılı S-kutusu) kullanılarak bu yöntemlerin çalışma yapılarını gösteren diyagramlar ve örnekler ortaya konmuştur.

Beşinci bölümde, şifreleme ve deşifreleme uygulamalarının gerçekleştirildiği MATLAB® GUI programıyla oluşturulan yazılım aracının özelliklerinden bahsedilmiştir.

Altıncı bölümde, yazılım aracı kullanılarak metin, görüntü, ses ve video çoklu ortam verilerinin her biri için şifreleme ve deşifreleme uygulamaları gerçekleştirilmiş ve yazılım aracında bulunan kaotik sistemlerden elde edilen rastgele sayıların rastgelelik testleri, yapılan şifreleme ve deşifreleme uygulamalarının aşamaları, şifreleme işlemlerinin analiz sonuçları ile sonuç değerleri hakkında detaylı yorumlamalar yapılmıştır.

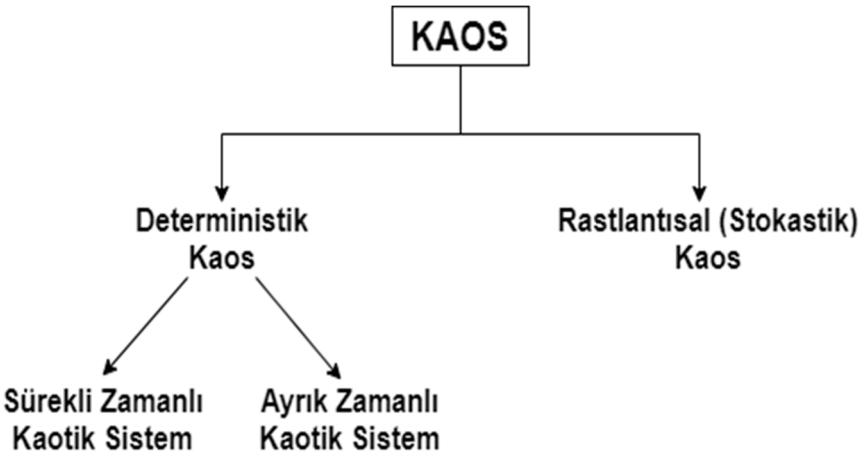
Tezin yedinci bölümü ise Sonuç ve Önerileri içermektedir.

BÖLÜM 2. KAOS

Kaos, doğada ve laboratuvar ortamında gözlemlenen, çeşitli uygulamalarda da kullanılan büyüleyici bir fenomendir. 1960'lardan beri matematik, fizik, biyoloji, kimya ve mühendislik gibi birçok farklı araştırma alanından gelen çalışmalarla geliştirilmiştir. Kaosun en iyi bilinen özelliği deterministik denklemler tarafından üretilen kaotik yörüngelerin zaman geçtikçe tamamen öngörülemeyen hale gelmesidir. Bu durum kelebek etkisi olarak adlandırılır.

Kaos, düzensiz ve rastgele gibi bir görünümde olan fakat aslında kendine has bir düzene sahip olan ve doğrusal olmayan durumları açıklayan bir bilim dalıdır. Başka bir tanım olarak kaos, dinamik sistemlerde bilinen en karmaşık kararlı hal davranışıdır. Kaosun ve kaotik işaretlerin başlıca önemli özellikleri; başlangıç şartlarına karşı hassas duyarlı olması, zaman boyutunda oluşan düzensizliği, sınırsız sayıda değişik periyodik salınımlar içermesi, limit kümesinin parçalı boyutlu olması, genliği ve frekansı tespit edilemeyen ancak sınırlı bir alanda değişen işaretler içermesidir [1].

Şekil 2.1'de belirtildiği gibi kaos, deterministik ve rastlantısal olarak iki durumda incelenebilir. Bilimin daha çok incelediği kısım deterministik kaos durumudur.



Şekil 2.1. Kaos durumları

2.1. Kaotik Sistemler

Kaotik sistemler, zaman içerisinde bir önceki adımın sonucunda elde edilen çıkış değerinin bir sonraki adım için giriş değeri olarak kullanıldığı geri beslemeli dinamik sistemlerdir. Bu sistemler, o anda bulunan durumu, geçmişteki durumlar cinsinden belirten bir kuralla birlikte olası durumların kümesini içerir. Sistemde bulunan değişkenler arasında doğrusal bir bağ bulunmadığından dolayı giriş ve çıkış değerleri arasındaki bağ orantılı değildir. Sistem üzerindeki tüm değişkenlerde girdinin sürekli olarak değişerek farklı düzenler yaratması ve devamında bu düzenlerin yine kendisini etkilemesi kaos olarak nitelendirilmektedir.

Kaotik sistemler matematiksel model olarak ayrık zamanlı sistemler ve sürekli zamanlı sistemler olarak iki bölüme ayrılırlar.

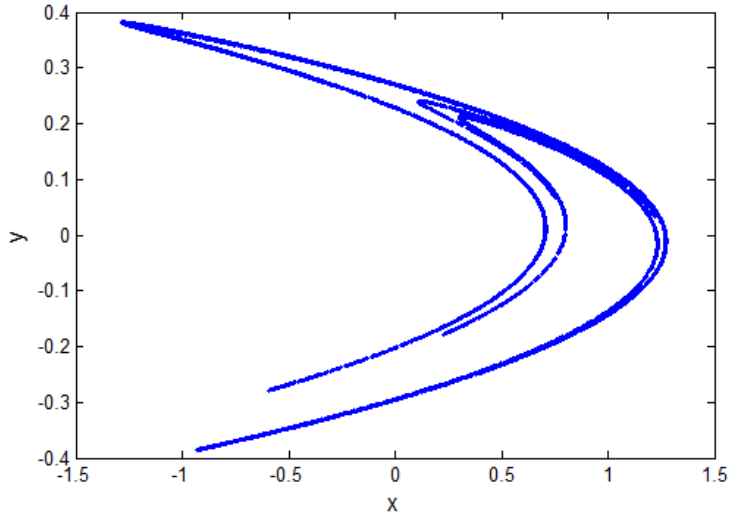
2.1.1. Ayrık zamanlı sistemler

Uygun doğrusal olmayan bir $f(x)$ fonksiyonunun iterasyonu sonucu oluşan genelde geri besleme yapan kaotik özellikli dizilerin oluşturduğu bir sistemdir. Bu sistemlerin genel olarak gösterimi denklem 2.1'de verilmiştir.

$$x_{n+1} = f(x_n) \tag{2.1}$$

Seçilen $f(x)$ fonksiyonun kaotik olması için fonksiyonun başlangıç şartlarına yüksek duyarlılık göstermesi gerekmektedir. Yani x_n değerlerinin çok farklı değerler alması gerekmektedir. Ayrık zamanlı sistemlerde genellikle bir ve iki boyutlu basit bir denklem ile bu davranış elde edilebilir.

Ayrık zamanlı kaotik sitemlere dair literatüre eklenen birçok çalışma yapılmıştır. Tek boyutlu ayrık zamanlı kaotik sistemlere Cubic Map [30] ile Tent Map [31] sistemleri örnek olarak verilebilir. Çift boyutlu ayrık zamanlı kaotik sistemlere ise Henon Map [32] ile Arnold's Cat Map [33] sistemleri örnek olarak gösterilebilir. Şekil 2.2'de Henon çekicisine ait görüntü verilmiştir.



Şekil 2.2. Henon çekicisine ait görüntü

2.1.2. Sürekli zamanlı sistemler

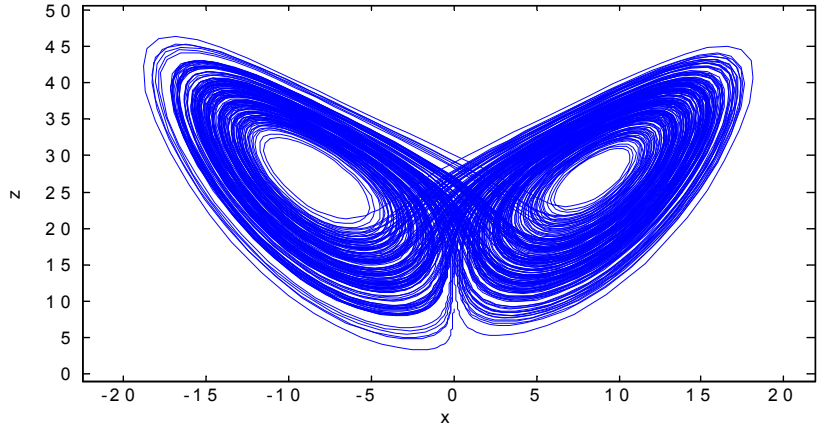
Sürekli zamanlı bir sistem, başlangıç durumu $\vec{x}(t_0) = \vec{x}_0$ olarak denklem 2.2'de gösterildiği gibi tanımlanabilir.

$$\frac{d\vec{x}(t)}{dt} = \vec{F}[\vec{x}(t), t] \tag{2.2}$$

Bu denklemde $\vec{F}: R^m \rightarrow R^m$ tanımlı vektör alanı olmak üzere; $\vec{x} \in R^m$ durum vektörü, $\vec{x}_0$ başlangıç durum vektörü, t zamanı ve t_0 ise başlangıç zamanı değerlerini gösterir. Denklem 2.2'de verilen tanımlı vektör alanı zamana bağımlı olmasından dolayı otonom olmayan bir sistemdir. Zamana bağımlı olmayan dinamik bir sistem ise otonom olan bir sistemdir [34]. Otonom sistem, başlangıç durumu $\vec{x}(t_0) = \vec{x}_0$ olmak üzere denklem 2.3 şeklinde tanımlanabilir.

$$\frac{d\vec{x}(t)}{dt} = \vec{F}[\vec{x}(t)] \tag{2.3}$$

Literatürde bulunan sürekli zamanlı kaotik sistemlere Lorenz [2], Rucklidge [35] ve Van Der Pol [36] sistemleri örnek olarak verilebilir. Şekil 2.3'te Lorenz sisteminin x-z faz portresi verilmiştir.



Şekil 2.3. Lorenz sisteminin x-z faz portresi

2.2. Kaos Analizleri

Bir dinamik sistemin kaos davranışında bulunup bulunmadığı yapılacak bazı analizlerle gösterilebilir. Bu analizlerin bir kısmı bu bölümde tanıtılacaktır.

2.2.1. Denge noktaları ve özdeğerler

Denge noktaları kaotik sistemlerde sistemin davranışı ile ilgili bilgi verir. Kaotik bir sistemin denge noktaları, $dx(t)/dt = F[x(t)] = 0$ eşitliği kullanılarak bulunur. Bu eşitliğin sonucunda elde edilen reel sayı değerleri denge noktalarının yerini belirtir. Bulunan denge noktaları etrafındaki çözümlerin davranışını da gösterir [37]. Bunun dışında bazı kaotik sistemlerin denge noktaları mevcut değildir. Eğer bir kaotik sistemde $dx(t)/dt = F[x(t)] = 0$ eşitliği sonucunda reel sayı değerleri yerine irreel sayı değerleri elde ediliyorsa o sistemin gerçek denge noktaları yoktur.

Kaotik dinamik sistemler kararsız bir davranış gösterirler. Dinamik sistemin özdeğerlerinden en az bir tanesi pozitif ise dinamik sistem kararsızdır. İlk olarak, özdeğerlerin bulunabilmesi için kullanılan Jakobiyen matrisinin denklem 2.4'te verildiği gibi bulunması gerekir.

$$J = \begin{bmatrix} \partial F_1/\partial x_1 & \partial F_1/\partial x_2 & \cdots & \partial F_1/\partial x_n \\ \partial F_2/\partial x_1 & \partial F_1/\partial x_2 & \cdots & \partial F_2/\partial x_n \\ \vdots & \vdots & \ddots & \vdots \\ \partial F_n/\partial x_1 & \partial F_n/\partial x_2 & \cdots & \partial F_n/\partial x_n \end{bmatrix} \tag{2.4}$$

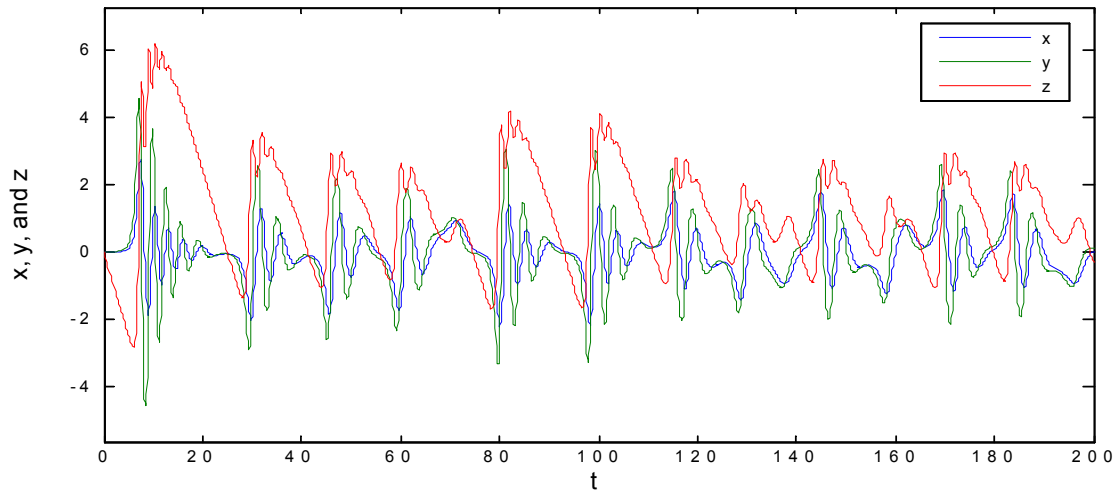
Jakobiyen matrisinin denklem 2.5'te kullanılmasıyla özdeğerler (λ) hesaplanır.

$$\det(J - \lambda I) = |J - \lambda I| = 0 \tag{2.5}$$

Denklem 2.5'te I, birim matris değerini temsil etmektedir. Denklemden elde edilen özdeğerler ile sistemin kararsızlığıyla ilgili yorum yapılabilir. Bulunan özdeğerlerden en az bir tanesinin reel kısmı pozitif bir değerde ise denge noktası kararsız olup sistemin kaotik olduğu sonucuna varılabilir. Fakat elde edilen özdeğerlerle sistemin kaos durumunda bulunup bulunmadığıyla ilgili bir kesinliğe ulaşılamaz. Sistemin kaotikliği konusunda daha doğru bir yargıya varılabilmesi için başka analizlerin de yapılması gerekmektedir [34].

2.2.2. Faz portreleri

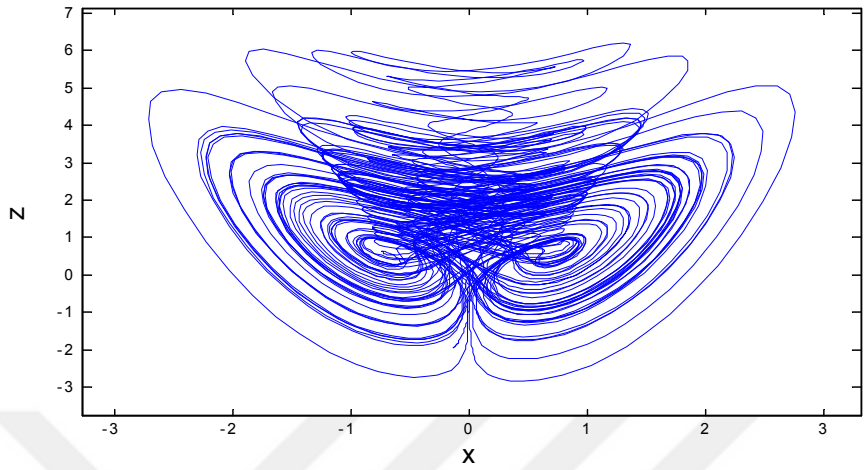
Kaotik sistemde bulunan durum değişkenleri değerlerinin zamana göre aperiyodik bir davranış sergilemesi beklenir. Bu değişkenlerin zamana göre oluşturdukları davranışlar gözlemlenerek bu durumun var olup olmadığı anlaşılabilir [38]. Şekil 2.4'te 3 boyutlu kaotik bir sistemin durum değişkenlerinin zamana göre göstermiş olduğu davranışlar verilmiştir.



Şekil 2.4. 3 boyutlu kaotik bir sistemin durum değişkenlerinin zamana göre değişimi

Kaotik sistemlerin durum değişkenlerinin birbirlerine göre olan davranışları gözlemlendiğinde belirli sınırlar içerisinde bulunan karmaşık görünümlü şekiller

oluşmaktadır. Bu, sistemin kaos durumunda bulunduğunu gösterir. Örnek olarak Pehlivan kaotik sisteminin [1] x ve z durum değişkenlerinin faz portresi Şekil 2.5'te verilmiştir.



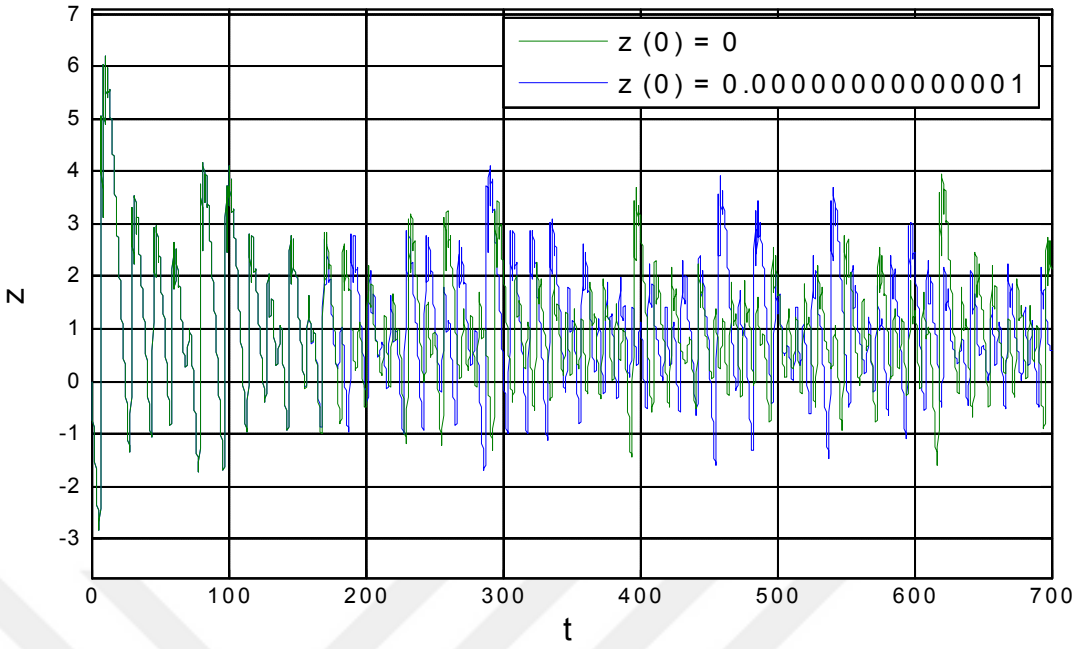
Şekil 2.5. Örnek kaotik sistemin 2 boyutlu faz portresi

2.2.3. Başlangıç şartlarına hassas duyarlılık analizi

Kaotik sistemlerin özelliklerinden birisi de başlangıç şartlarına karşı hassas duyarlılık göstermeleridir. Sistemin durum değişkenlerinden herhangi birisinin başlangıç değerinin değişmesi, sistemin bütün durum değişkenlerinin çözüm kümesini yani tüm girdi ve çıktı değerlerini değiştirir. Kaotik sistemin durum değişkenlerinden bir tanesinin iki farklı başlangıç değeriyle aynı sistem için çözdürülmesi sonucu elde edilen çıkış değerlerinden sistemin başlangıç şartlarına olan hassas duyarlılığı gözlemlenebilir. Bu durum için denklem 2.6'da bulunan Pehlivan kaotik sistemi kullanılarak bir örnek verilmiştir.

$$\begin{cases} \dfrac{dx}{dt} = \mathrm{y} - \mathrm{x} \\ \dfrac{dy}{dt} = a * y - x * z \\ \dfrac{dz}{dt} = x * y - a \end{cases} \tag{2.6}$$

Denklem 2.6'da verilen Pehlivan kaotik sisteminde bulunan parametre $a = 0.5$ ve başlangıç şartları $x_0 = 0.001$, $y_0 = 0.001$, $z_0 = 0$'dır. Sadece z fazının başlangıç değeri $z_0 = 10^{-14}$ olarak değiştirilip sistem yeniden çözdürülürse iki z fazının çıkış değerlerinin zamana göre oluşan grafikleri Şekil 2.6'da gösterildiği gibi çizdirilir.



Şekil 2.6. Örnek sistemin başlangıç şartlarına olan hassas duyarlılığını gösteren zaman serileri

2.2.4. Lyapunov üstelleri

Bir dinamik sistemin başlangıç şartlarına hassas duyarlılığı ve sistemin karakteristik özellikleriyle ilgili bilgiler Lyapunov üstelleri ile belirlenir. Bu üsteller kaotik bir sistemin davranışının da bir ölçüsüdür.

Dinamik bir sistemin davranışı başlangıç şartlarına karşı hassas duyarlılık gösteriyorsa zaman ilerledikçe faz uzayındaki birbirine yakın olan yörüngeler hızlıca birbirinden ayrılır ve sistem kararsız olamaya başlar. Lyapunov üsteli faz uzayında oluşan komşu eğrilerin yerel ayrılma derecelerinin ortalamasıdır [39].

Denklem 2.7'den birinci Lyapunov üstel değeri λ;

$$\lambda = \frac{1}{t_N - t_0} \sum_{k=1}^{N} \log_2 \frac{d(t_k)}{d(t_{k-1})} \tag{2.7}$$

şeklinde hesaplanır. Bu denklemdeki $d(t)$ uzaklık değeridir. İki başlangıç değeri arasındaki uzaklık d_0 olmak üzere daha sonraki bir zamanda uzaklık, denklem 2.8'deki gibi ifade edilir.

$$d(t) = d_0 e^{\lambda t} \tag{2.8}$$

Üç boyutlu sürekli zamanlı sistemlerde kaotik davranışı belirten tek durum "–, 0, +" durumudur ($\lambda_1 < 0, \lambda_2 = 0, \lambda_3 > 0$) [40]. Dört boyutlu sistemlerde ise Lyapunov üstellerin işaretlerine göre üç farklı şekilde kaos durumu oluşur.

- Lyapunov üstelleri (+, +, 0, –) ise bu sistem hiperkaos,
- Lyapunov üstelleri (+, 0, –, –) ise bu sistem kaos (tuhaf çekici),
- Lyapunov üstelleri (+, 0, 0, –) ise bu sistem torus kaostur.

Üç ve dört boyutlu sistemlerde kaos durumu oluşturmayan diğer Lyapunov üstel durumları Tablo 2.1'de verilmiştir.

Tablo 2.1. Lyapunov üstellerin işaretlerine göre durumları

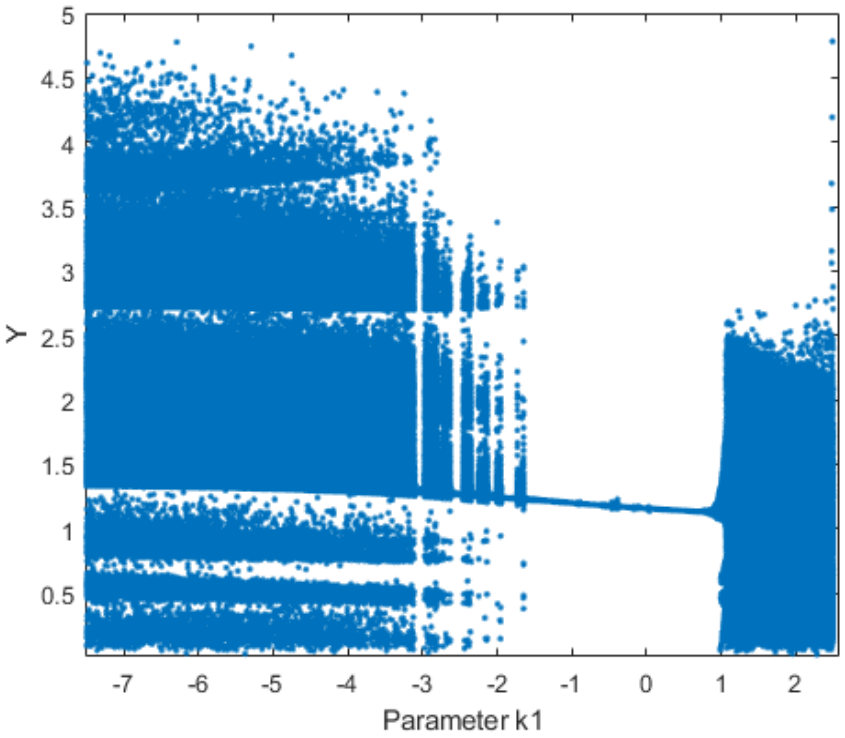
Sistem Derecesi	**Sistem Durumları**	**Lyapunov Üstellerin İşaretleri**
3 Boyutlu Sistemler	Sabit Nokta	(-,-,-)
	Limit Döngü	(0,-,-)
	Torus	(0,0,-)
	Tuhaf Çekici	(-,0,+)
4 Boyutlu Sistemler	Sabit Nokta	(-,-,-,-)
	Limit Döngü	(0,-,-,-)
	Torus	(+,0,0,-)
	Tuhaf Çekici	(+,0,-,-)
	Hiperkaos	(+,+,0,-)

2.2.5. Çatallaşma diyagramı

Dinamik sistemi oluşturan denklemlerdeki durum değişkenleri, denklem içerisinde bulunan parametrelerin değişimine göre farklı değerler alırlar. Çatallaşma, dinamik sistemlerde meydana gelen sistem parametrelerindeki en ufak değişimlerin faz uzaylarındaki yapısal değişimlerine karşılık gelmesi durumudur [1,41]. Bu tarz değişiklikler sistemin kararlılığını etkilemektedir. Dinamik sistemin bir parametresinin belirli aralıklarda olan değerlerine göre sistem durum değişkeninin yerel maksimum

değerlerinin birbirlerine göre çizdirilmesi ile çatallaşma diyagramı elde edilir. Bu diyagram kullanılarak sistemin kaotikliği ve kararlılığı gibi özellikleri hakkında yorum yapılabilir [34].

Hu5d kaotik sisteminin $k1$ parametresi için elde edilen çatallaşma diyagramı Şekil 2.7'de verilmiştir [42]. Şekil 2.7'de, $k1$ parametresi -7.5 ile 2.5 aralığında iken durum değişkeni olan y'nin aldığı değerler gösterilmektedir. Buna göre $k1$ parametresi -7.5 ile -1.5 aralığında iken sistem birden fazla kez kaos durumunda bulunup bu durumdan çıkmıştır. $k1$ parametresi 0.8 ile 2.5 değerleri arasındayken de sistemin sürekli olarak kaos durumunda bulunduğu gözlemlenir.



Şekil 2.7. Örnek bir çatallaşma diyagramı

2.3. Referans Kaotik Sistemler

Kaotik sistemler diferansiyel denklemler ile tanımlanmaktadır. Kaotik sistemlerin tanımlandığı bu diferansiyel denklemlerin sayısal tabanlı olarak modellenebilmesi için sayısal analiz yöntemleri kullanılmaktadır. Bu yöntemlere Euler, Heun, 4. ve 5. dereceden Runge-Kutta (RK4 ve RK5) yöntemleri örnek olarak gösterilebilir.

Bu tez çalışmasında kaotik sistemlerin çözdürülmesinde literatürde de en çok tercih edilen sayısal analiz yöntemlerinden birisi olan RK4 yöntemi kullanılmaktadır. Sayısal analizde Runge-Kutta yöntemleri, adi diferansiyel denklemlerin çözüm yaklaşımları için kapalı ve açık yinelemeli yöntemler ailesinin önemli bir parçasıdır [34]. Denklem 2.9'da bir başlangıç değer problemi sunulmuştur.

$$y' = f(t, y), \qquad y(t_0) = y_0 \tag{2.9}$$

RK4 yönteminin bu problem için uygulanışı denklem 2.10 ile gerçekleştirilir.

$$y_{n+1} = y_n + \frac{1}{6}(k_1 + 2k_2 + 2k_3 + k_4) \tag{2.10}$$

Denklem 2.10'da bulunan k değerleri aşağıda bulunan dört denklem ile hesaplanır.

$$k_1 = hf(t_n, y_n) \tag{2.11}$$

$$k_2 = hf\left(t_n + \frac{h}{2}, y_n + \frac{k_1}{2}\right) \tag{2.12}$$

$$k_3 = hf\left(t_n + \frac{h}{2}, y_n + \frac{k_2}{2}\right) \tag{2.13}$$

$$k_4 = hf(t_n + h, y_n + k_3) \tag{2.14}$$

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

- k_1, aralığın başlangıcında olan eğimdir.
- k_2, aralığın orta noktasında olan eğimdir. k_2 eğimi, Euler Yöntemi kullanılarak y'nin $t_n + h/2$ noktasındaki değerinden elde edilir.
- k_3, yine orta noktadaki eğimdir.
- k_4 ise aralığın sonunda olan eğimdir [34].

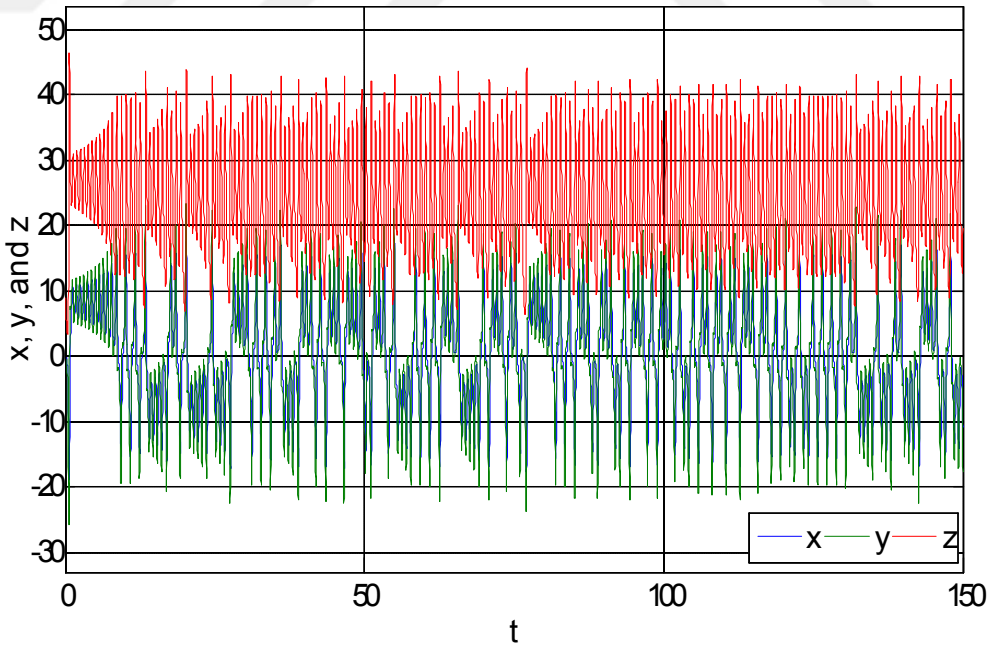
Oluşturulan yazılım aracının içerisinde bulunan ve uygulamalarda kullanılan referans kaotik sistemler, sistemlerin başlangıç şartları ile parametre değerleri ve sistemlerin RK4'e göre çözdürülmesi sonucu oluşan zaman serileri ile faz portreleri her kaotik sistemin tanıtıldığı bölümde verilmiştir.

2.3.1. Lorenz sistemi

Lorenz, 1963 yılında meteorolog olarak çalışmalar gerçekleştirirken üç değişkenli bir sistemde başlangıç şartlarında oluşan çok küçük değişimlerin belirli bir süre sonunda tahmin edilemeyen sonuçlar doğurabileceğini göstermiştir. Yapılan bu çalışma kaos biliminin başlangıcı olarak kabul edilir. Lorenz kaotik sistem modeli denklem 2.15 ile ifade edilir [2].

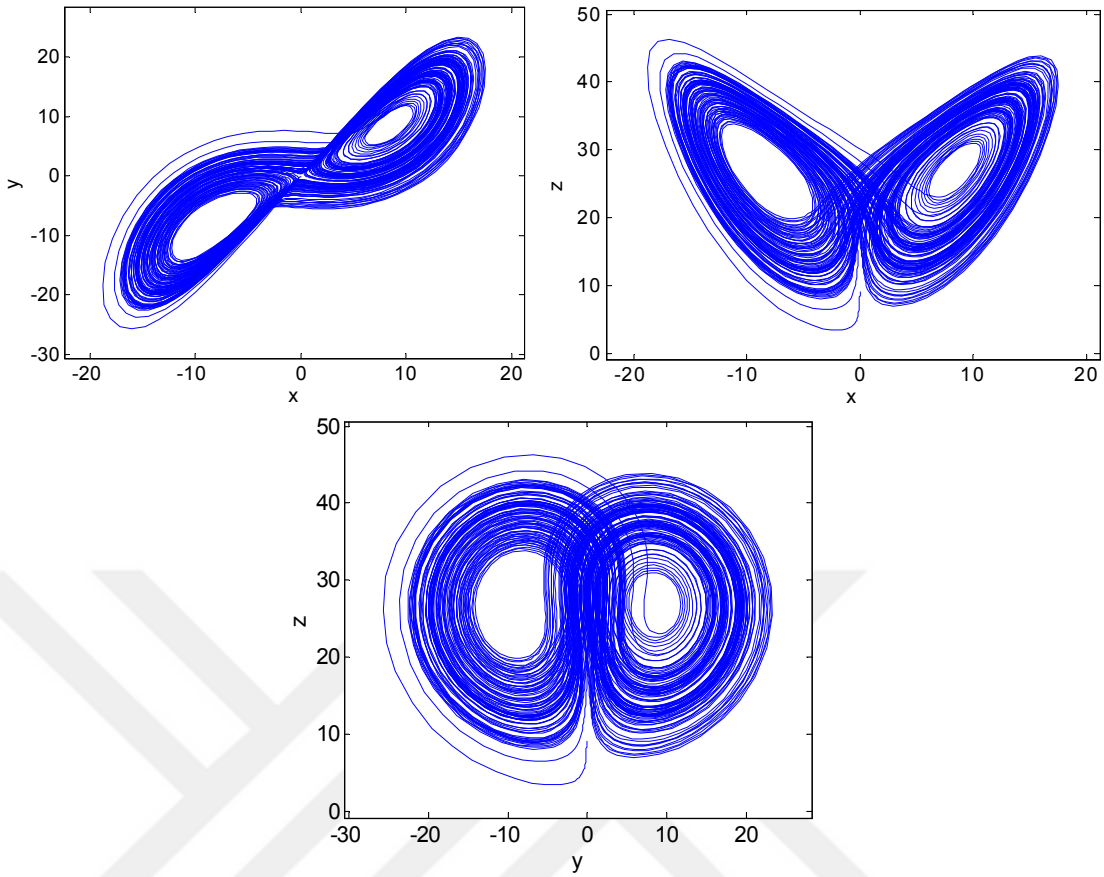
$$\begin{cases} \frac{dx}{dt} = \sigma * (y - x) \\ \frac{dy}{dt} = x * (\rho - z) - y \\ \frac{dz}{dt} = x * y - (\beta * z) \end{cases} \tag{2.15}$$

Sistem 3 boyutludur. Sabit parametreler σ = 10, β = 8/3, ρ = 28 ve başlangıç şartları $x_0 = 0$, $y_0 = -0.1$, $z_0 = 9$ olmak üzere sistemden elde edilen zaman serisi Şekil 2.8'de verilmiştir.



Şekil 2.8. Lorenz sisteminin faz değerleri - zaman grafiği

Zaman serisinin bulunmasından sonra Lorenz kaotik sisteminin 2 boyutlu faz portreleri ise Şekil 2.9'daki gibi elde edilir.



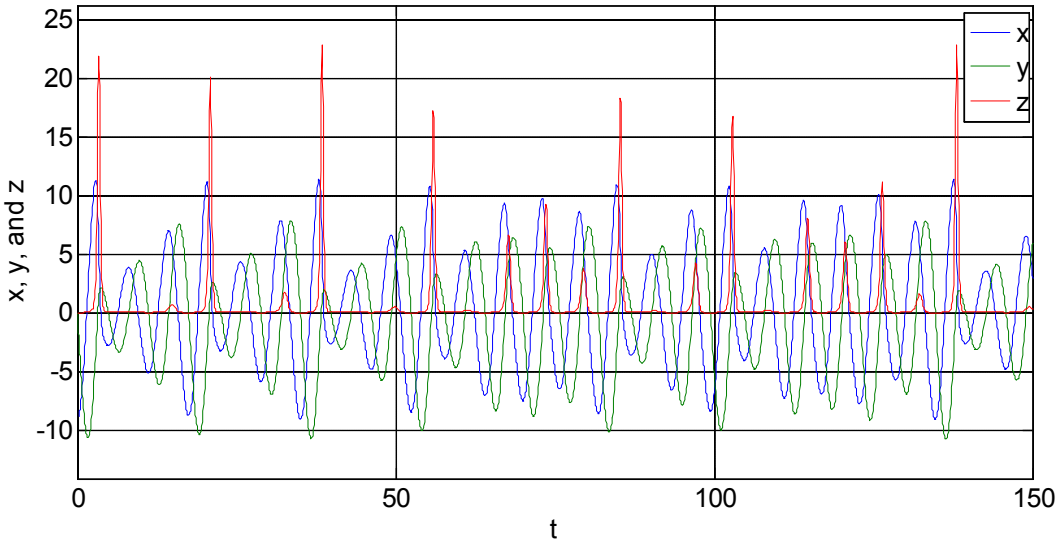
Şekil 2.9. Lorenz sistemi faz portreleri

2.3.2. Rössler sistemi

Rössler tarafından bulunan bu kaotik sistem kimyasal reaksiyonların incelenmesiyle oluşturulmuştur. Rössler kaotik sistem modeli denklem 2.16 ile ifade edilir [43].

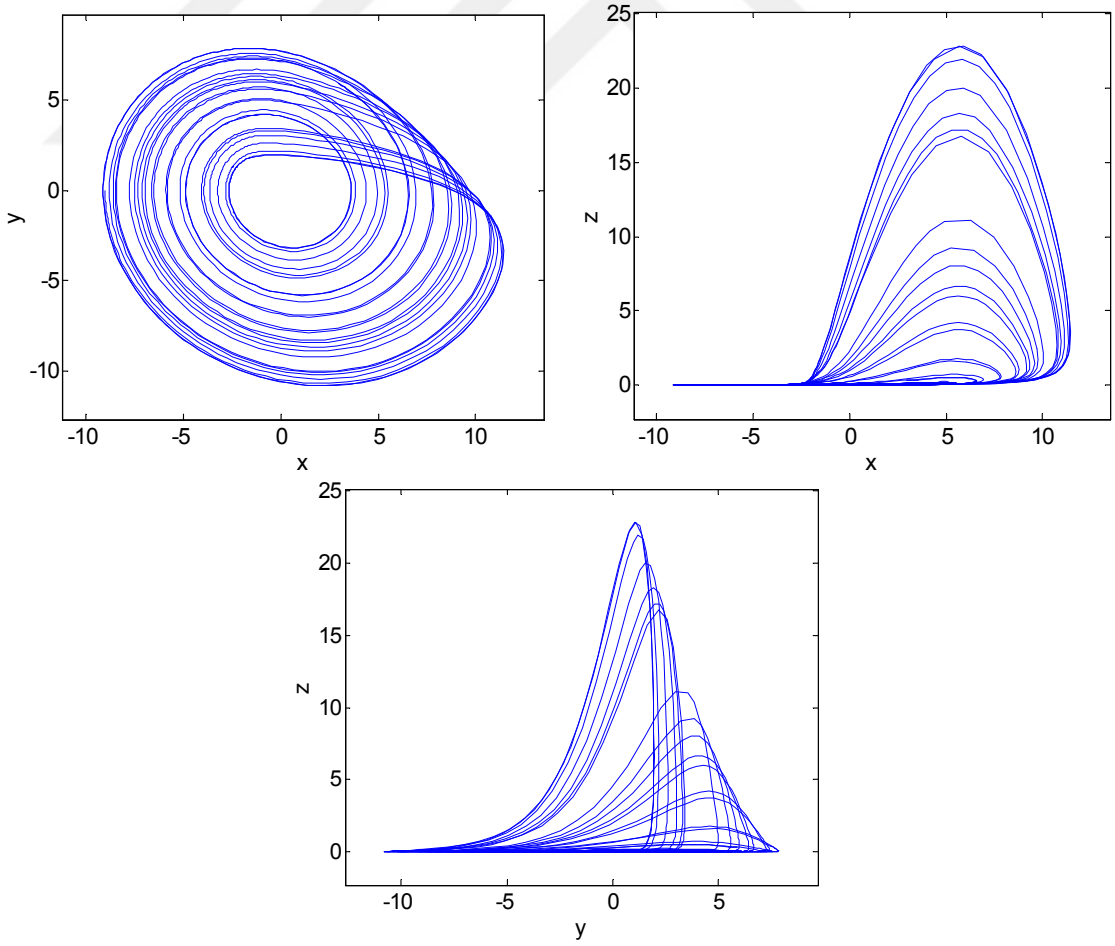
$$\begin{cases} \dfrac{dx}{dt} = -y - z \\ \dfrac{dy}{dt} = x + a * y \\ \dfrac{dz}{dt} = b + z * (x - c) \end{cases} \tag{2.16}$$

Sistem 3 boyutludur. Sabit parametreler $a = 2$, $b = 2$, $c = 5.7$ ve başlangıç şartları $x_0 = -9$, $y_0 = 0$, $z_0 = 0$ olmak üzere sistemden elde edilen zaman serisi Şekil 2.10'da verilmiştir.



Şekil 2.10. Rössler sisteminin faz değerleri - zaman grafiği

Zaman serisinin bulunmasından sonra Rössler kaotik sisteminin 2 boyutlu faz portreleri ise Şekil 2.11'deki gibi elde edilir.



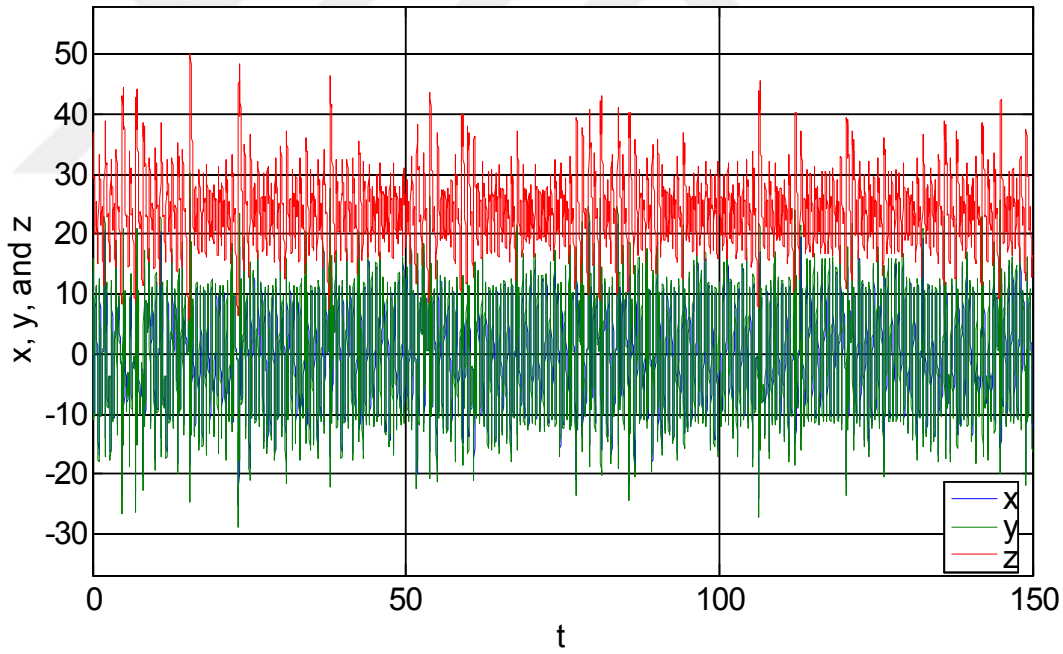
Şekil 2.11. Rössler sistemi faz portreleri

2.3.3. Chen sistemi

1999 yılında Chen ve Ueta tarafından literatüre kazandırılan Chen kaotik sistem modeli denklem 2.17 ile ifade edilir [44].

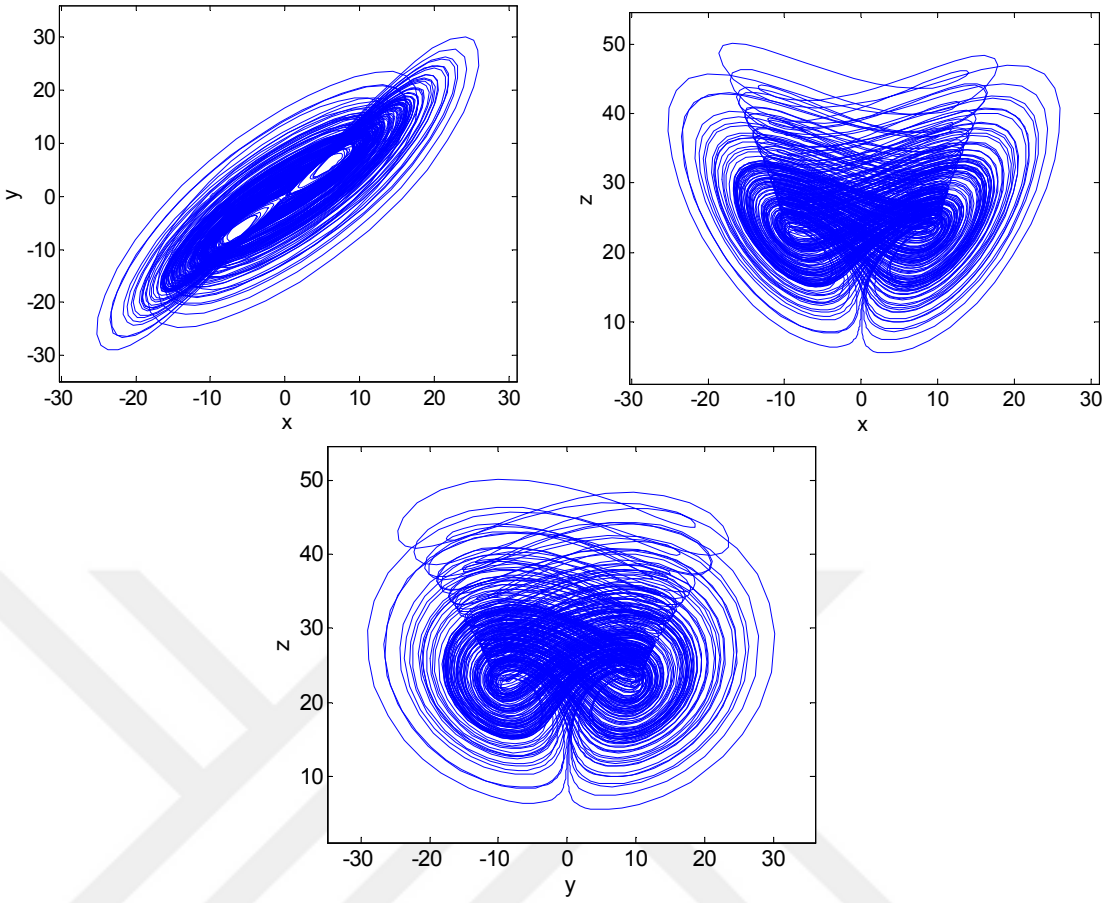
$$\begin{cases} \frac{dx}{dt} = a * (y - x) \\ \frac{dy}{dt} = (c - a) * x - x * z + c * y \\ \frac{dz}{dt} = x * y - b * z \end{cases} \tag{2.17}$$

Sistem 3 boyutludur. Sabit parametreler $a = 35$, $b = 3$, $c = 28$ ve başlangıç şartları $x_0 = -10, y_0 = 0, z_0 = 37$ olmak üzere sistemden elde edilen zaman serisi Şekil 2.12'de verilmiştir.



Şekil 2.12. Chen sisteminin faz değerleri - zaman grafiği

Zaman serisinin bulunmasından sonra Chen kaotik sisteminin 2 boyutlu faz portreleri ise Şekil 2.13'deki gibi elde edilir.



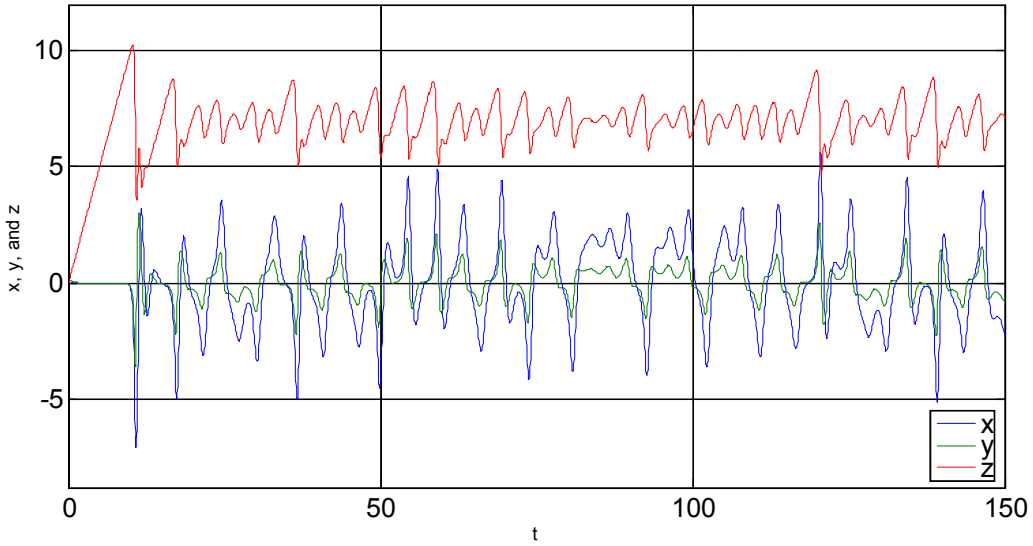
Şekil 2.13. Chen sistemi faz portreleri

2.3.4. Rikitake sistemi

Rikitake sistemi, dünyanın jeomanyetik alanının düzensiz polarite anahtarlamasını açıklamaya çalışan bir modeldir. Rikitake kaotik sistem modeli denklem 2.18 ile ifade edilir [45].

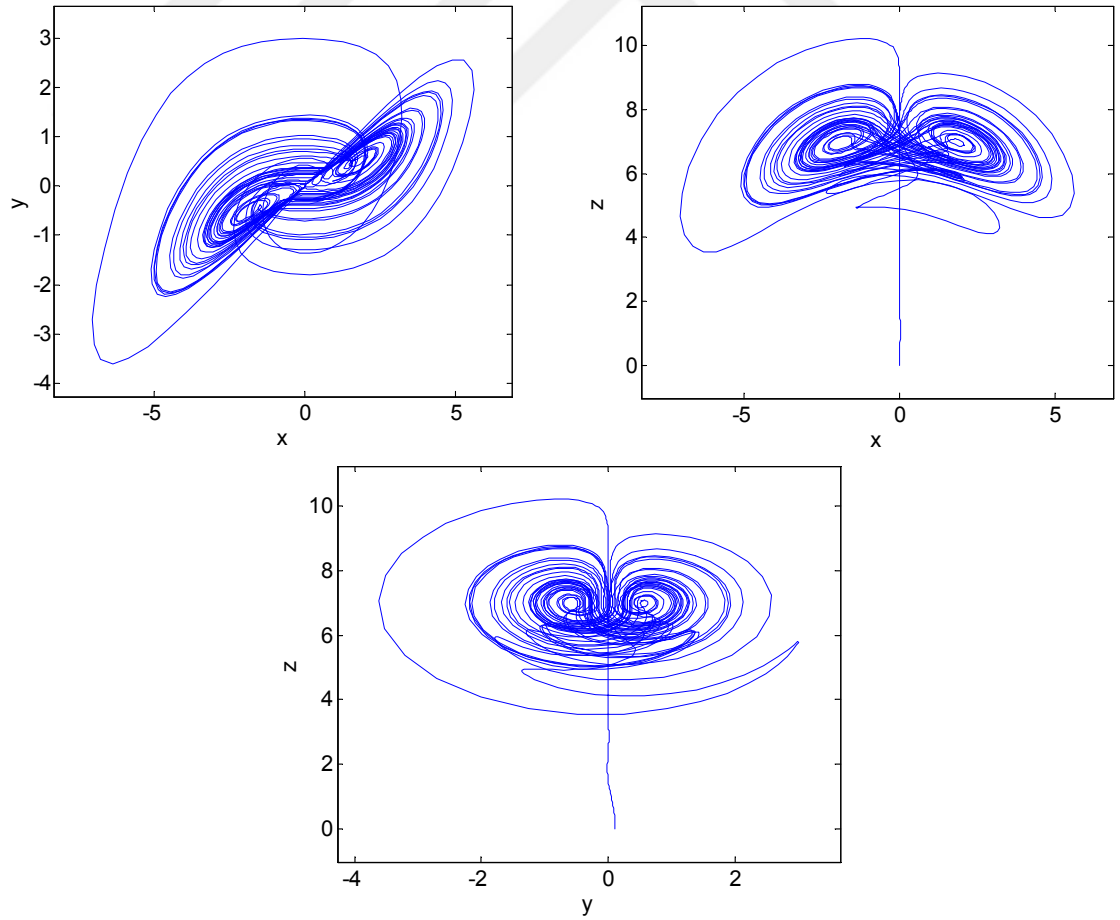
$$\begin{cases} \dfrac{dx}{dt} = -\mu * x + z * y \\ \dfrac{dy}{dt} = -\mu * x + (z - a) * x \\ \dfrac{dz}{dt} = 1 - x * y \end{cases} \tag{2.18}$$

Sistem 3 boyutludur. Sabit parametreler $\mu = 2$, $a = 5$ ve başlangıç şartları $x_0 = 0$, $y_0 = 0.1, z_0 = 0$ olmak üzere sistemden elde edilen zaman serisi Şekil 2.14'te verilmiştir.



Şekil 2.14. Rikitake sisteminin faz değerleri - zaman grafiği

Zaman serisinin bulunmasından sonra Rikitake kaotik sisteminin 2 boyutlu faz portreleri ise Şekil 2.15'deki gibi elde edilir.



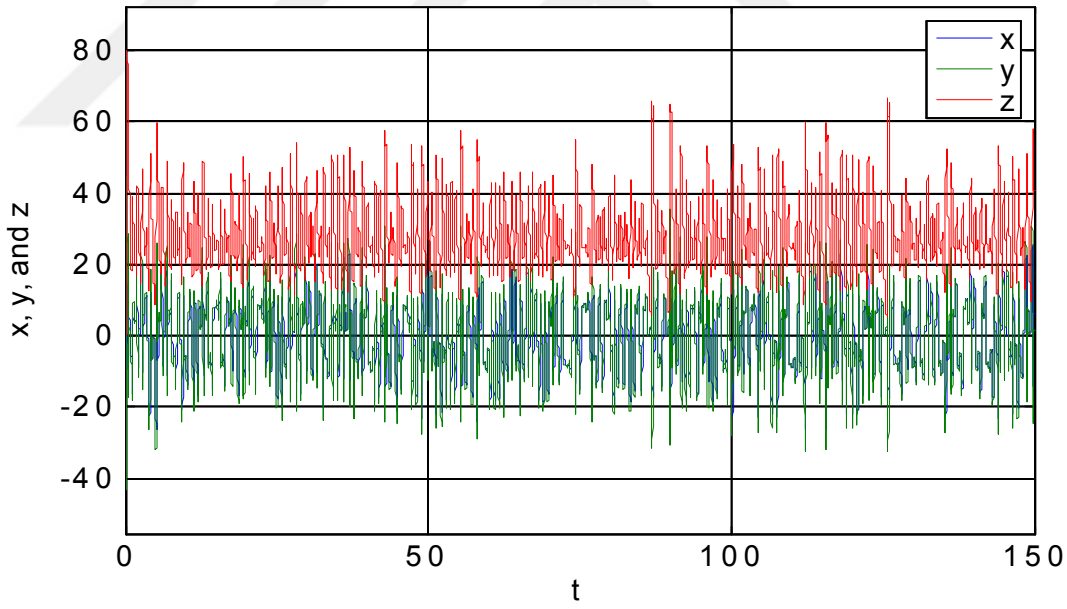
Şekil 2.15. Rikitake sistemi faz portreleri

2.3.5. Cai sistemi

Cai ve Tan bulmuş oldukları bu sistemin doğrusal olmayan kontrol yolu kullanarak senkronizasyonunu incelemişlerdir. Cai kaotik sistem modeli denklem 2.19 ile ifade edilir [46].

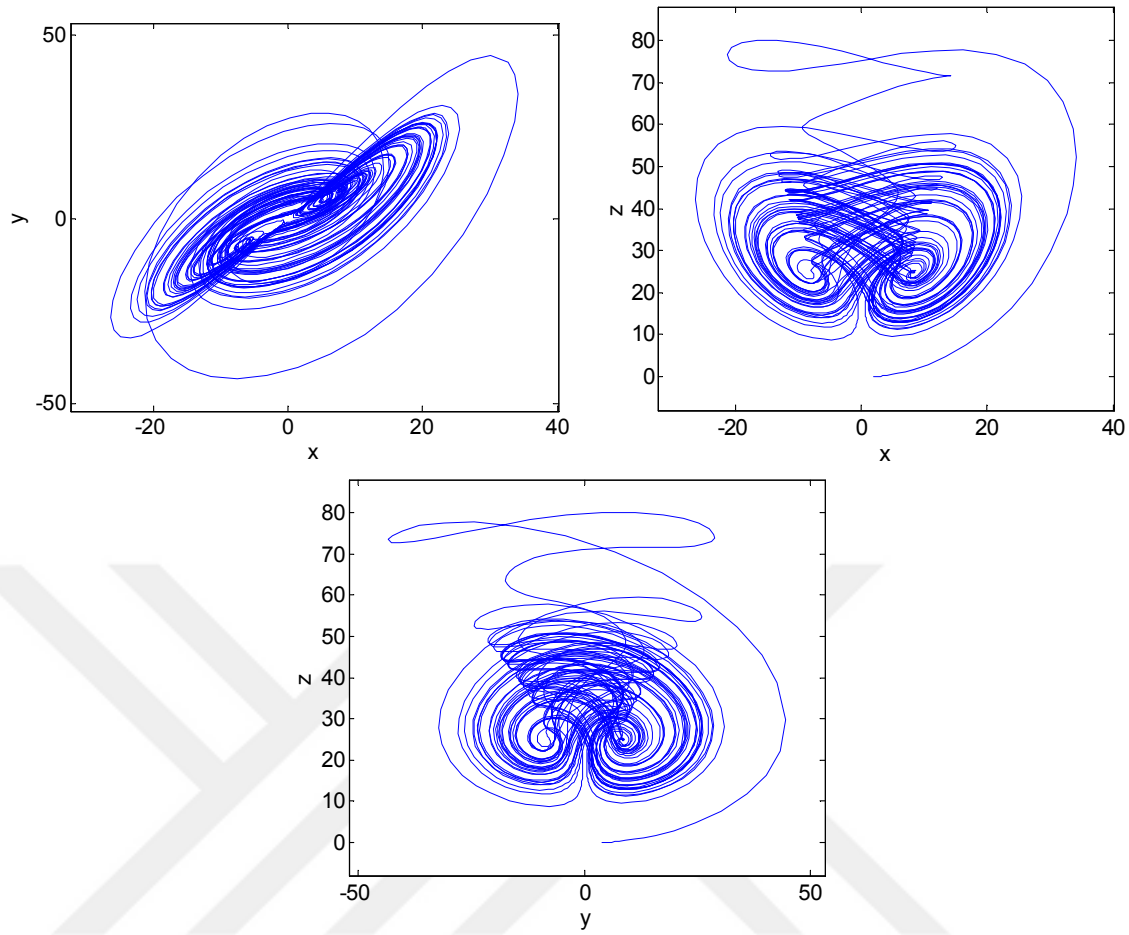
$$\begin{cases} \frac{dx}{dt} = a * (y - x) \\ \frac{dy}{dt} = b * x + c * y - x * z \\ \frac{dz}{dt} = x^3 - h * z \end{cases} \tag{2.19}$$

Sistem 3 boyutludur. Sabit parametreler a = 20, b = 14, c =10.6, h = 2.8 ve başlangıç şartları $x_0 = 2$, $y_0 = 4$, $z_0 = 0$ olmak üzere sistemden elde edilen zaman serisi Şekil 2.16'da verilmiştir.



Şekil 2.16. Cai sisteminin faz değerleri - zaman grafiği

Zaman serisinin bulunmasından sonra Cai kaotik sisteminin 2 boyutlu faz portreleri ise Şekil 2.17'deki gibi elde edilir.



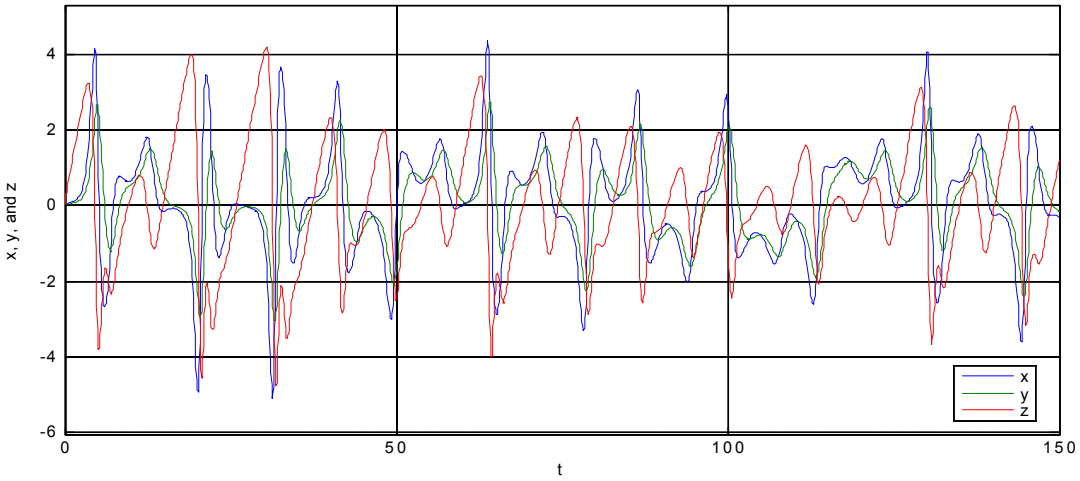
Şekil 2.17. Cai sistemi faz portreleri

2.3.6. Sprott94b sistemi

Sprott, 1994 yılında yapmış olduğu çalışmada 19 tane üç boyutlu otonom kaotik sistem önermiştir. Sprott94b kaotik sistem modeli de bu denklemlerden birisidir. Sprott94b kaotik sistem modeli denklem 2.20 ile ifade edilir [47].

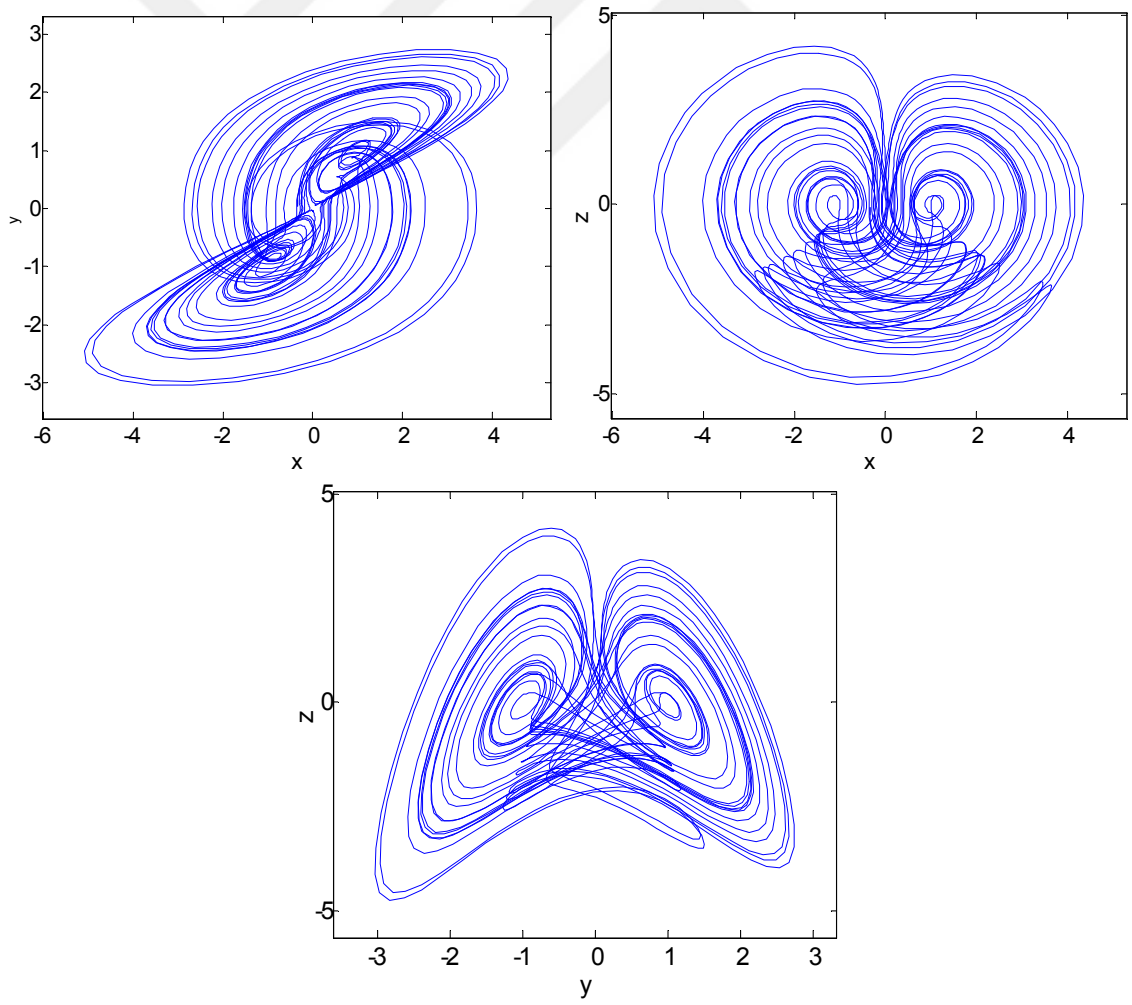
$$\begin{cases} \frac{dx}{dt} = y * z \\ \frac{dy}{dt} = x - y \\ \frac{dz}{dt} = 1 - x * y \end{cases} \tag{2.20}$$

Sistem 3 boyutludur. Başlangıç şartları $x_0 = 0.05$, $y_0 = 0.05$, $z_0 = 0.05$ olmak üzere sistemden elde edilen zaman serisi Şekil 2.18'de verilmiştir.



Şekil 2.18. Sprott94b sisteminin faz değerleri - zaman grafiği

Zaman serisinin bulunmasından sonra Sprott94b kaotik sisteminin 2 boyutlu faz portreleri ise Şekil 2.19'daki gibi elde edilir.



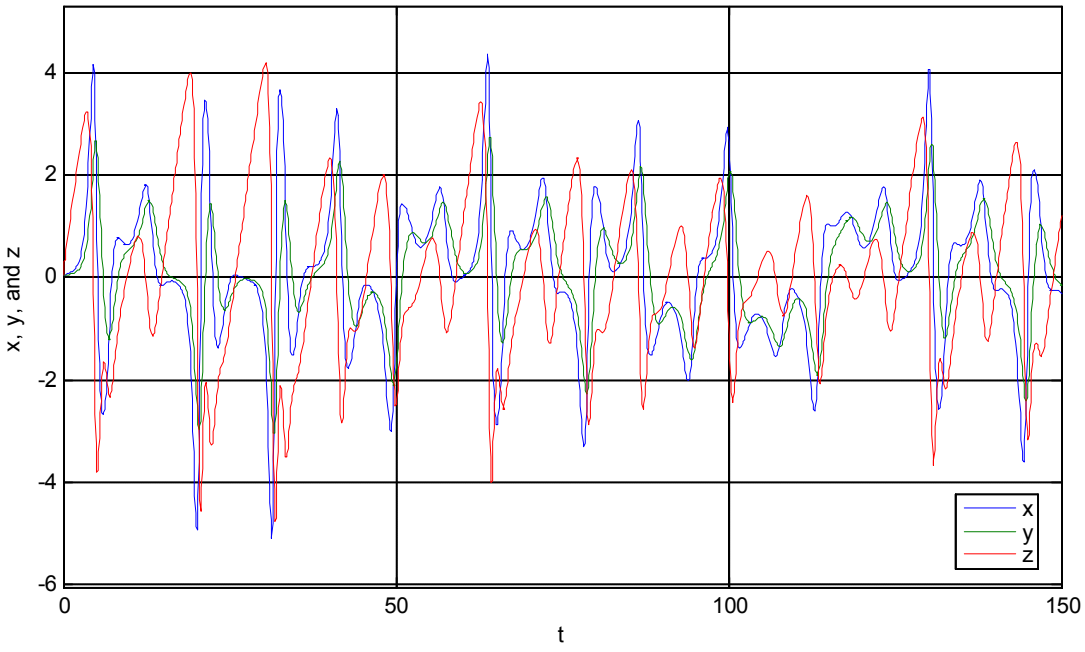
Şekil 2.19. Sprott94b sistemi faz portreleri

2.3.7. Sundarapandian sistemi

2012 yılında Sundarapandian ve Pehlivan tarafından literatüre kazandırılan Sundarapandian kaotik sistem modeli denklem 2.21 ile ifade edilir [48].

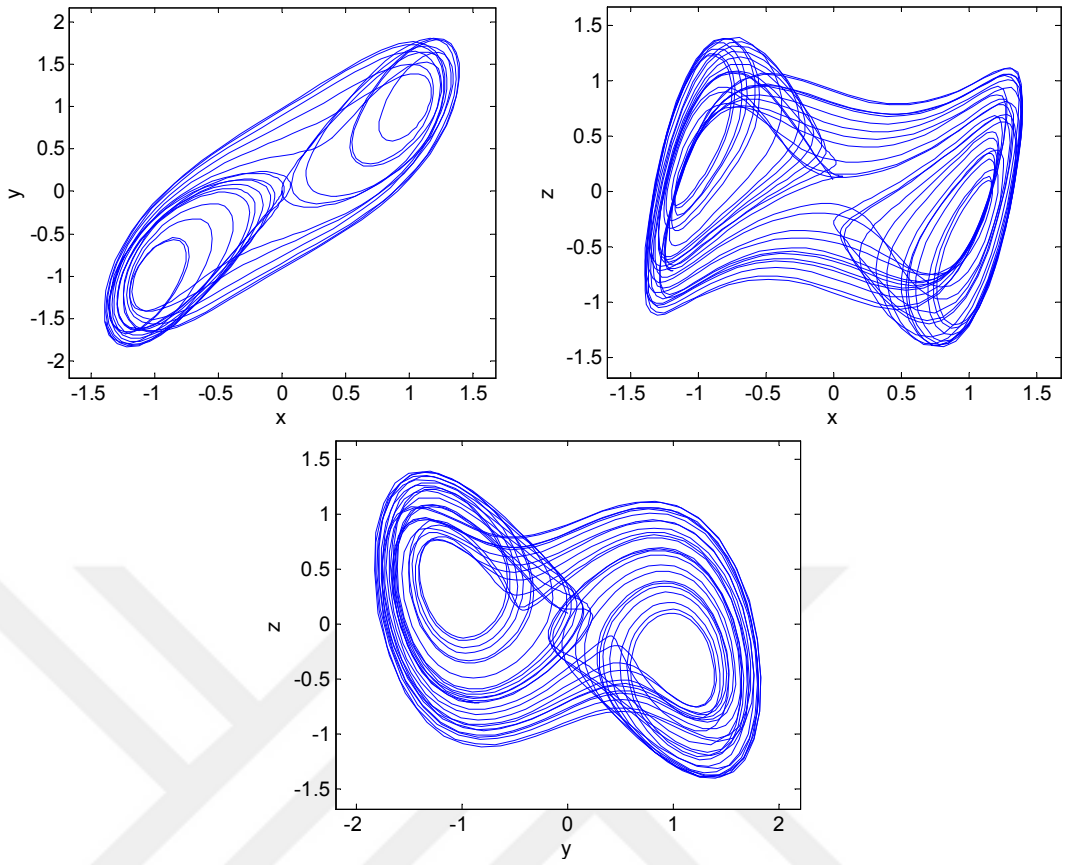
$$\begin{cases} \frac{dx}{dt} = a * y - x \\ \frac{dy}{dt} = -b * x - z \\ \frac{dz}{dt} = c * z + x * y * y - x \end{cases} \tag{2.21}$$

Sistem 3 boyutludur. Sabit parametreler a = 1, b = 0.46, c= 0.46 ve başlangıç şartları $x_0 = 0$, $y_0 = 0$, $z_0 = 0.1$ olmak üzere sistemden elde edilen zaman serisi Şekil 2.20'de verilmiştir.



Şekil 2.20. Sundarapandian sisteminin faz değerleri - zaman grafiği

Zaman serisinin bulunmasından sonra Sundarapandian kaotik sisteminin 2 boyutlu faz portreleri ise Şekil 2.21'deki gibi elde edilir.



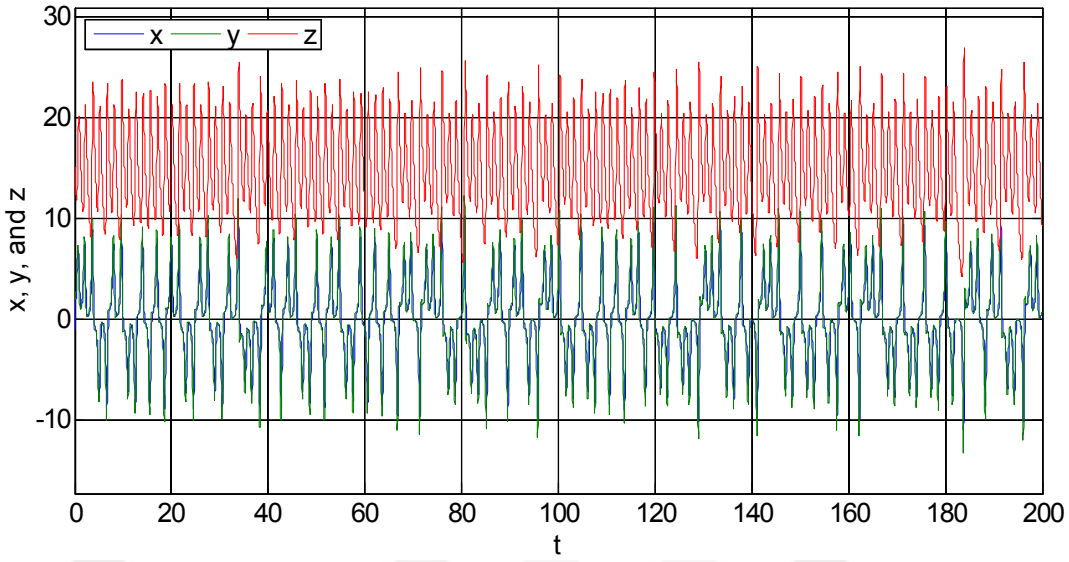
Şekil 2.21. Sundarapandian sistemi faz portreleri

2.3.8. Zhou sistemi

Zhou ve arkadaşları 2008 yılında Lorenz kaotik sistemini baz alarak yaptıkları çalışmayla literatüre kazandırdıkları Zhou sistemi denklem 2.22 ile ifade edilir [49].

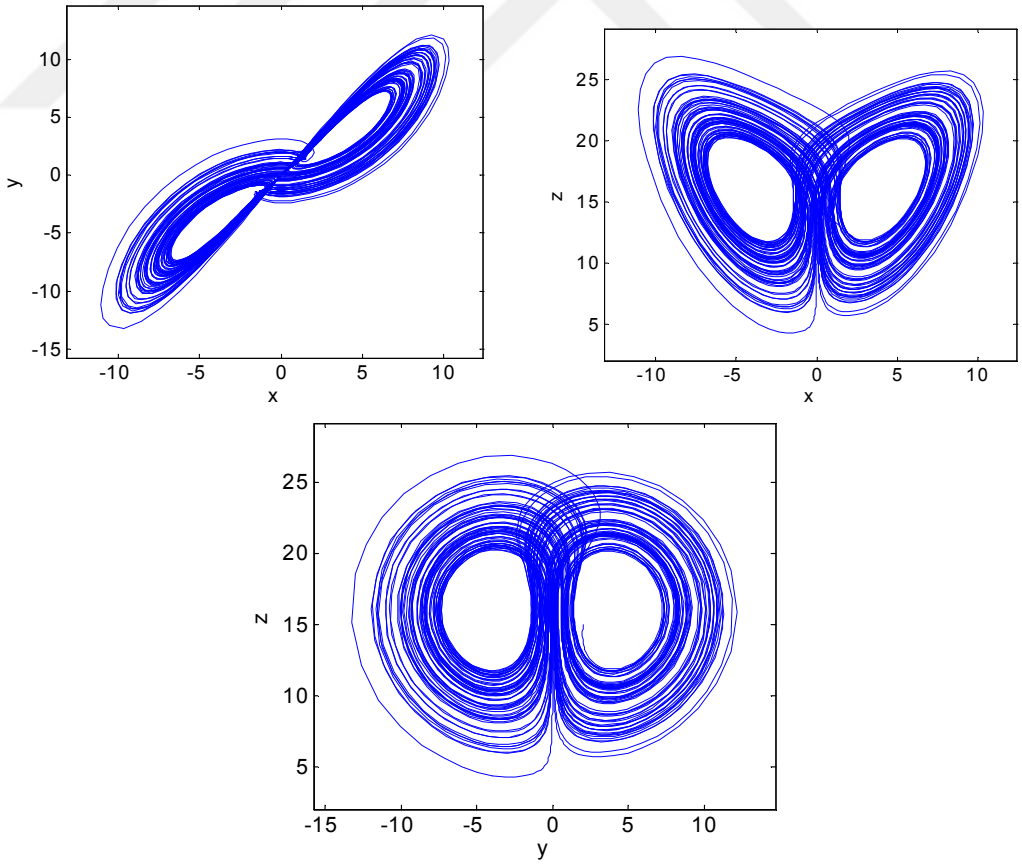
$$\begin{cases} \dfrac{dx}{dt} = a * (y - x) \\ \dfrac{dy}{dt} = b * x - x * z \\ \dfrac{dz}{dt} = x * y - z \end{cases} \tag{2.22}$$

Sistem 3 boyutludur. Sabit parametreler a = 10, b = 16 c = -1 ve başlangıç şartları $x_0 = -1, y_0 = 2, z_0 = 15$ olmak üzere sistemden elde edilen zaman serisi Şekil 2.22'de verilmiştir.



Şekil 2.22. Zhou sisteminin faz değerleri - zaman grafiği

Zaman serisinin bulunmasından sonra Zhou kaotik sisteminin 2 boyutlu faz portreleri ise Şekil 2.23'deki gibi elde edilir.



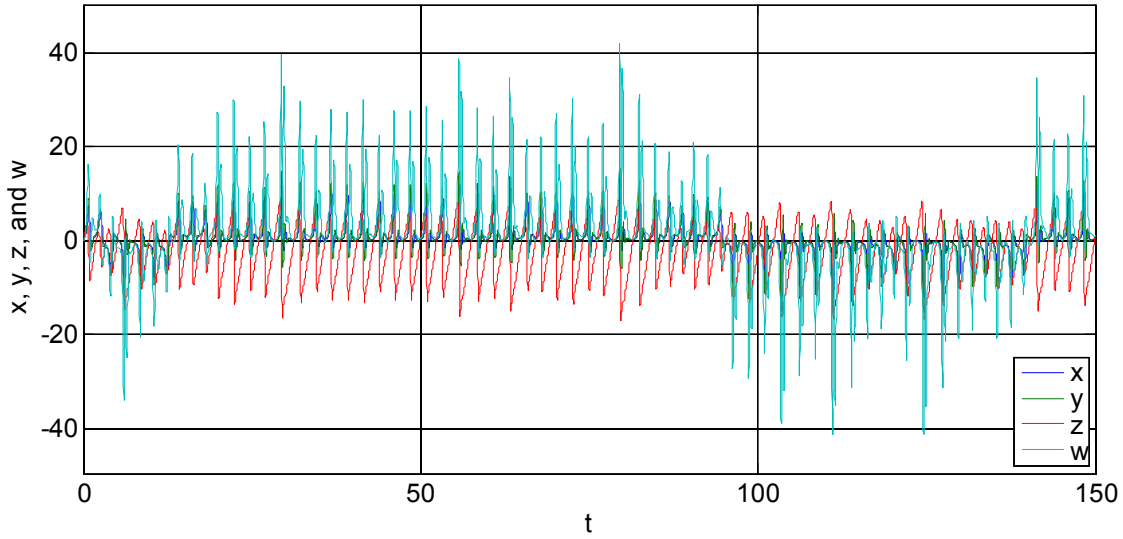
Şekil 2.23. Zhou sistemi faz portreleri

2.3.9. Lai4d sistemi

Lai ve arkadaşlarının 2018 yılında Sprott94b kaotik sistemini baz alarak yaptıkları çalışma ile literatüre kazandırdıkları Lai4d kaotik sistem modeli denklem 2.23 ile ifade edilir [50].

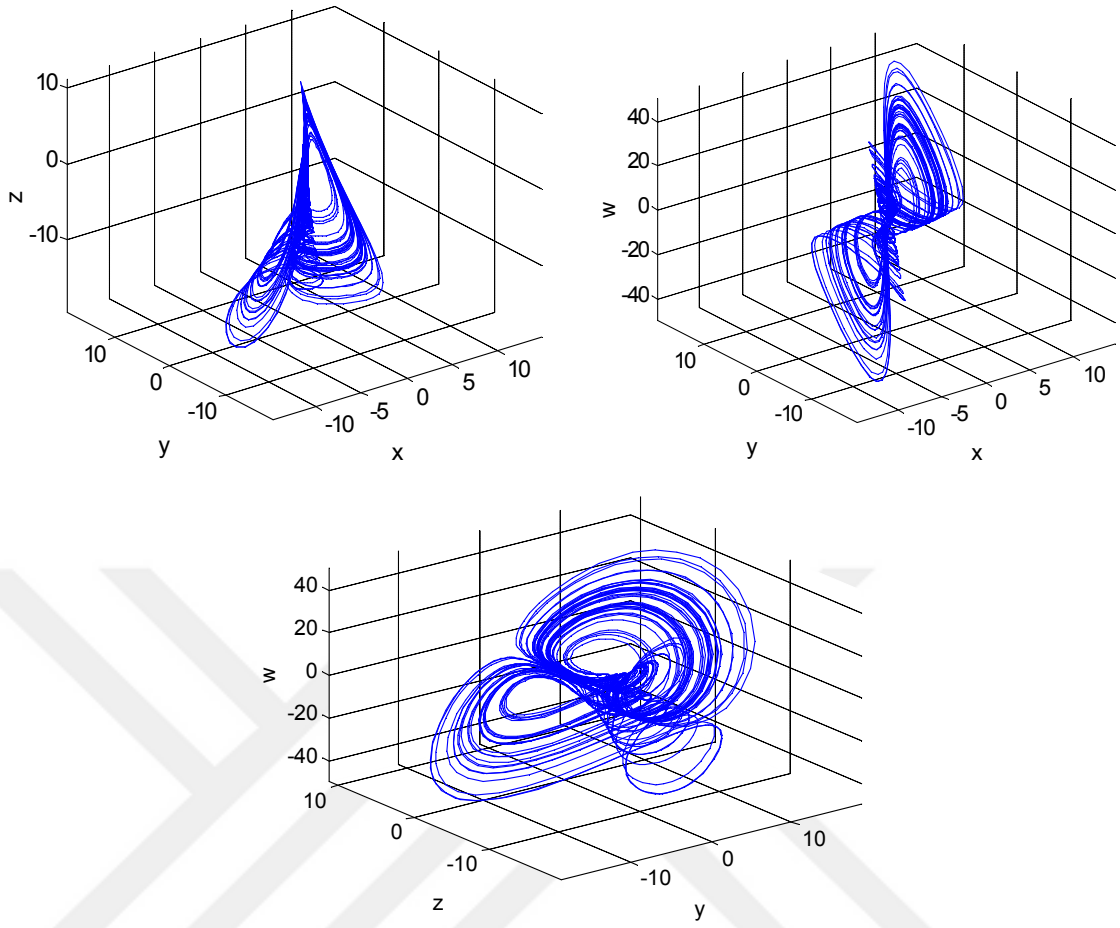
$$\begin{cases} \frac{dx}{dt} = a * (y - x) \\ \frac{dy}{dt} = x * z + w \\ \frac{dz}{dt} = b - x * y \\ \frac{dw}{dt} = c * y * z \end{cases} \tag{2.23}$$

Sistem 4 boyutludur. Sabit parametreler $a = 10$, $b = 10$ $c = 3$ ve başlangıç şartları $x_0 = 1$, $y_0 = 1$, $z_0 = 0$, $w_0 = 0$ olmak üzere elde edilen zaman serisi Şekil 2.24'te verilmiştir.



Şekil 2.24. Lai4d sisteminin faz değerleri - zaman grafiği

Zaman serisinin bulunmasından sonra Lai4d kaotik sisteminin 3 boyutlu faz portreleri ise Şekil 2.25'deki gibi elde edilir.



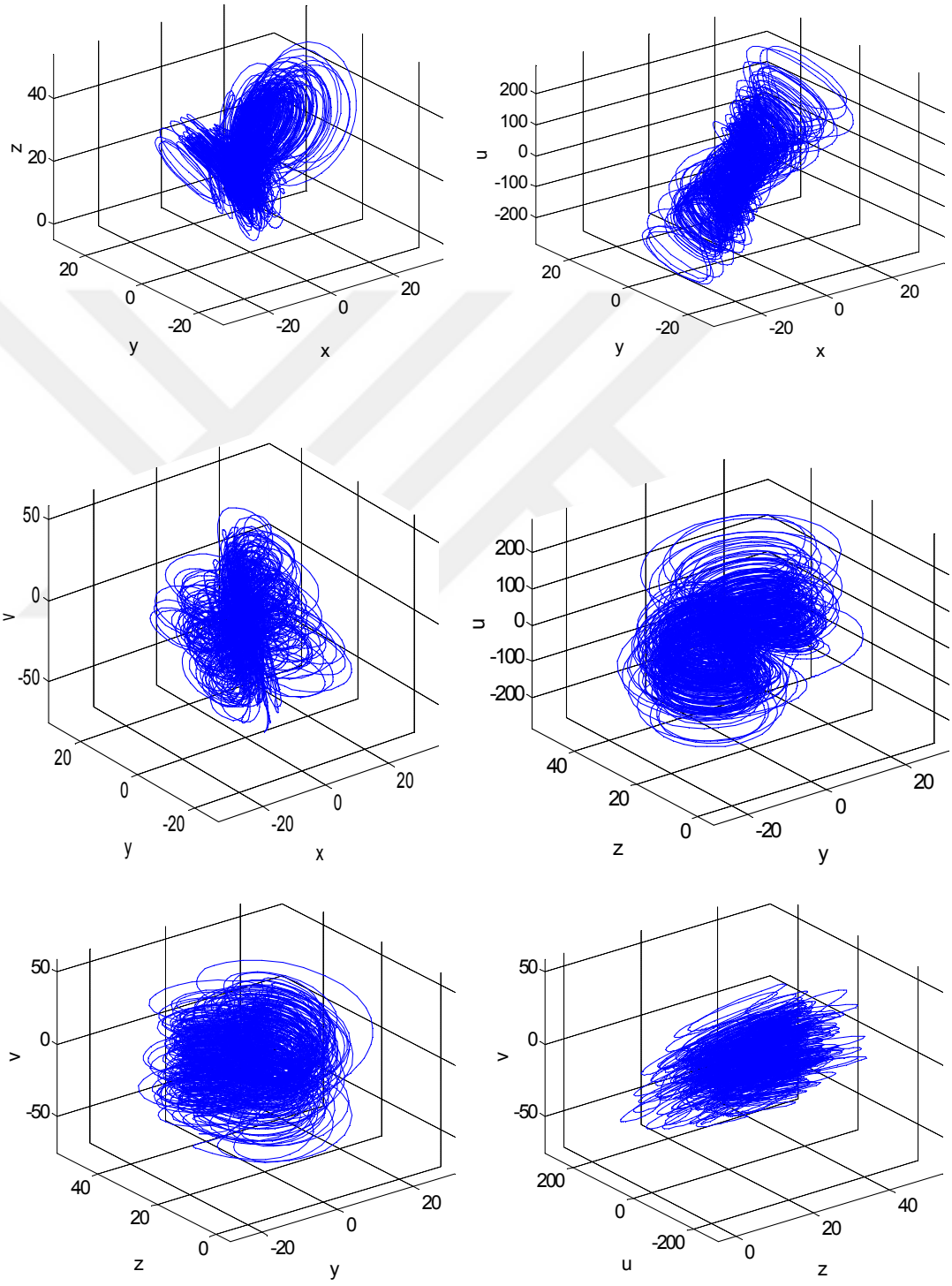
Şekil 2.25. Lai4d sistemi faz portreleri

2.3.10. Hu5d sistemi

Hu'nun 2008 yılında Lorenz kaotik sistemini baz alarak yapmış olduğu çalışmayla literatüre kazandırdığı Hu5d kaotik sistem modeli denklem 2.24 ile ifade edilir [51].

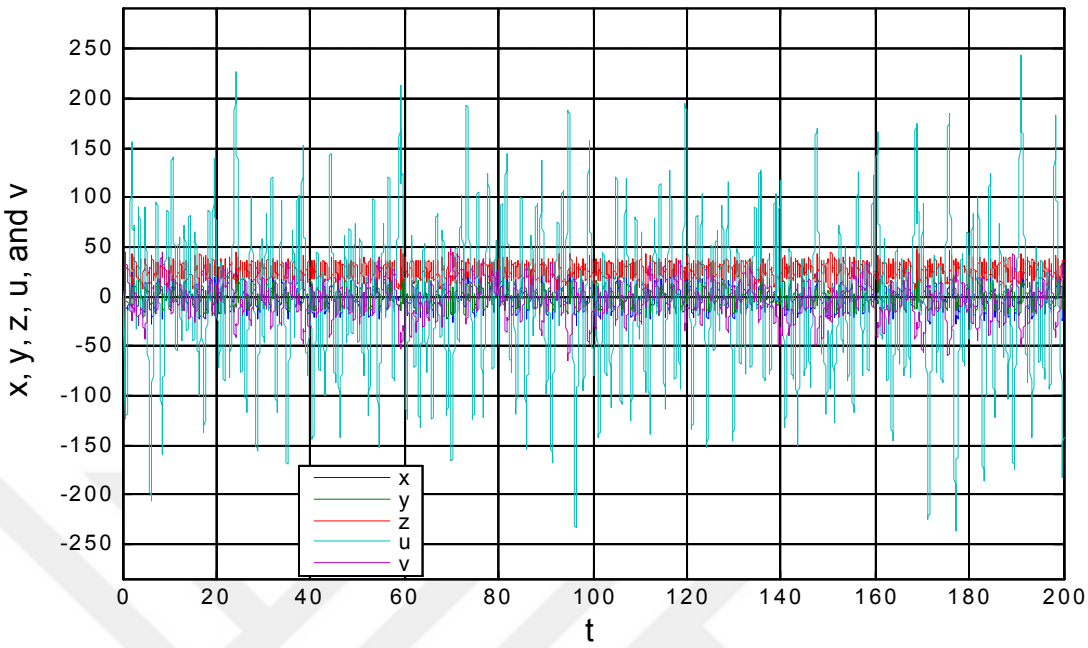
$$\begin{cases} \frac{dx}{dt} = \sigma * (y - x) + u \\ \frac{dy}{dt} = r * x - y - x * z - v \\ \frac{dz}{dt} = -\beta * z + x * y \\ \frac{du}{dt} = -\mathrm{x} * \mathrm{z} + \mathrm{k1} * \mathrm{u} \\ \frac{dv}{dt} = \mathrm{k2} * \mathrm{y} \end{cases} \tag{2.24}$$

Sistem 5 boyutludur. Sabit parametreler σ = 10, r = 28, β = 8/3, $k1$ = 2, $k2$ = 7.3 ve başlangıç şartları $x_0 = 0$, $y_0 = 0$, $z_0 = 0$, $u_0 = 2$, $v_0 = 2$ olmak üzere elde edilen 3 boyutlu faz portreleri Şekil 2.26'da verilmiştir.



Şekil 2.26. Hu5d sistemi faz portreleri

Hu5d kaotik sisteminden elde edilen zaman serisi ise Şekil 2.27'de verilmiştir.



Şekil 2.27. Hu5d sisteminin faz değerleri - zaman grafiği

BÖLÜM 3. KRİPTOLOJİ ve RASTGELE SAYI ÜRETECİ

Bu bölümde kriptoloji bilimi, RSÜ kavramları, şifreleme uygulamalarında kullanılacak rastgele sayıların elde edilmesi için tasarlanan rastgele sayı üreteçleri hakkında bilgiler verilmiş ve sayı dizilerinin rastgeleliğinin ölçülmesinde kullanılan testlerden biri olan NIST 800-22 testinin özelliklerinden bahsedilmiştir. Ayrıca tez çalışması kapsamında 6. bölümde gerçekleştirilen şifreleme uygulamalarının içerisinde bulunan güvenlik analizlerinin tanıtımı bu bölümde gerçekleştirilmiştir.

3.1. Kriptoloji

Kriptoloji, haberleşme gizliliğinin sağlanabilmesi, verilerin saklanması ve korunması durumları hakkında çalışan bir bilim dalıdır. Kriptoloji, kriptografi ve kriptoanaliz olarak iki bölüme ayrılır. Kriptografi verinin şifrelenmesi işlemidir. Çözümü çok zor olan matematik problemlerini ve sistemleri inceler. Kriptoanaliz de bu matematik problemlerini çözmeye çalışma veya şifreyi çözme işlemi olarak tanımlanabilir.

Bir haberleşme uygulamasında mesajı gönderen taraf gönderici, mesajın ulaştığı tarafsa alıcı olarak adlandırılır. Gönderici, gönderdiği verinin içeriğinin herhangi bir kişi tarafından görülmesini istemediğinden dolayı gönderdiği veriyi belirli bir sisteme göre değiştirme yani şifreleme yoluna başvurur. Alıcı da şifrelenmiş olan veriyi belirli bir sisteme göre çözüp orijinal haline geri getirerek deşifreleme işlemini gerçekleştirir. Şifrelenmemiş bilgiye "açık metin" denir. Açık metin herhangi bir formattaki veridir (Örneğin görüntü dosyası, ses dosyası). Açık metnin şifreleme algoritması kullanılarak herkesin anlayamayacağı şekle dönüştüğü bilgiye ise "şifreli metin" denir [14,52].

Haberleşme esnasında açık bir haberleşme kanalı kullanılıyorsa iletilen bilgiye istenmeyen üçüncü kişilerin erişebileceği, haberleşme kanalına girip bilginin içeriğini değiştirebileceği veya bozabileceği gibi durumlar problem oluşturur. Haberleşmede bilginin güvenli bir şekilde göndericiden alıcı tarafa ulaştığına emin olunmalıdır. Bu da

gönderilecek olan bilginin şifrelenmesi ile gerçekleştirilebilir. Böylelikle açık haberleşme kanallarında iletilen bilginin güvenli bir şekilde alıcı tarafa ulaştırılması sağlanır. Şifreleme uygulamaları matematiksel işlem temellerine dayanan bir yapıda çalışırlar. Şifreleme haberleşmeyi güvence altına alır ve bilginin bulunduğu kısımlara izinsiz olan girişleri engeller.

Modern şifre sistemleri 4 ana fonksiyonu sağlamak üzerine kuruludur:

- **Gizlilik:** Bilgi içeriğinin istenmeyen kişiler tarafından anlaşılmamasını sağlamaktır.
- **Bütünlük:** Bilginin saklanması durumunda veya gönderimi sırasında bilgi içeriğinin değiştirilmediğinden emin olunması gerekmektedir.
- **Reddedilemezlik:** Bilgiyi oluşturan ya da alıcıya gönderen kişi, daha sonra bu bilginin kendisi tarafından oluşturulduğunu veya gönderildiğini inkâr edememelidir.
- **Kimlik belirleme:** Gönderen ve alıcı taraflar birbirlerinin kimliklerini doğrulayabilmelidirler. Üçüncü bir kişinin başkasının kimliğine bürünme ihtimalinden dolayı alıcı taraf, gönderilen iletinin kaynağını araştırmak isteyebilmektedir.

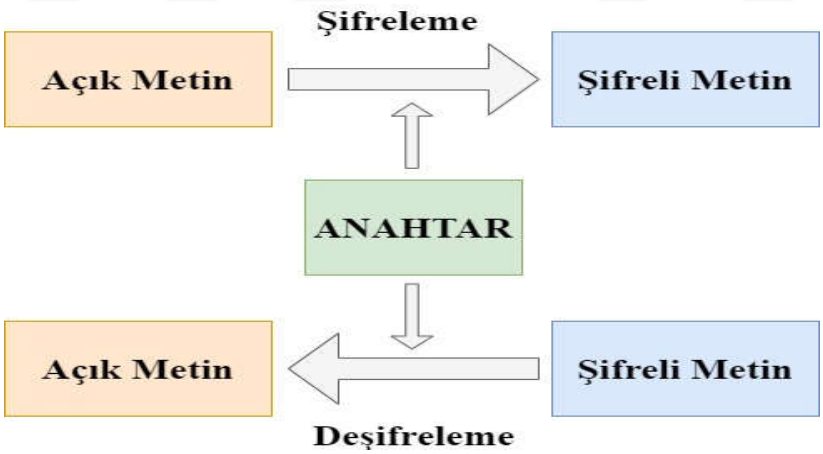
Modern şifreleme teknikleri, simetrik şifreleme ve asimetrik şifreleme olarak ikiye ayrılmaktadır. Bu iki teknik arasındaki temel fark şifreleme uygulamalarında kullanılacak olan anahtarların kullanım şeklidir. Bu iki şifreleme tekniği temel alınarak tasarlanan kaos tabanlı şifreleme yöntemleri de kriptografi uygulamalarında sıkça kullanılmaktadır. Bunun en önemli sebepleri kaotik sistemlerin başlangıç şartlarına karşı hassasiyet göstermesi ve doğrusallık göstermemesi özelliklerinin şifreleme uygulamalarından beklenen karıştırma ve yayılma özelliklerini sağlayabilmesidir [25,53].

3.1.1. Simetrik şifreleme

Simetrik şifrelemede şifreleme ve deşifreleme işlemlerinde aynı anahtar kullanılır. Bu anahtar gizli anahtar olarak adlandırılır. Gizli anahtar birbiri ile şifreli iletişim kurmak isteyen gönderici ve alıcı taraflarınca bilinmelidir. İletişimin güvenli olabilmesi için anahtarın gizli tutulması gerekmektedir. Simetrik şifreleme algoritmaları, asimetrik

şifreleme algoritmalarına göre daha hızlı çalışırlar. Simetrik şifreleme algoritmalarına AES, DES, Blowfish, IDEA ve RC4 algoritmaları örnek olarak verilebilir [54].

Simetrik şifreleme, iletişim kurmak isteyen taraflar arasında önceden paylaşılan ve gizli tutulması gereken tek bir anahtarın şifreleme ve deşifreleme işlemlerinde kullanılmasıyla iletişimin sağlandığı sistemlerdir. Bu sistem 5 adet bileşenden oluşur. Bu bileşenler; açık metin, şifreleme algoritması, gizli anahtar, şifrelenmiş metin ve deşifreleme algoritmasıdır. İlk bileşen olan açık metin şifreleme algoritmasıyla şifrelenecek olan mesaj ya da veridir. İkinci bileşen olan şifreleme algoritması açık metin içeriğinde yerine koyma ve dönüşüm işlemlerini uygular. Üçüncü bileşen olan gizli anahtar ise şifreleme algoritmasına açık metin gibi girdi olarak girer [55]. Anahtar, açık metin ve algoritmadan bağımsızdır. Kullanılan anahtara göre şifreleme algoritması farklı çıkış değerleri üretir. Dördüncü bileşen olan şifreli metin, açık metin ve gizli anahtara bağlı olarak üretilen karmaşık veri dizisidir. Son bileşen olan deşifreleme algoritması ise şifreli metin bilgisi ile gizli anahtar değerlerini kullanarak açık metin çıktısını tekrar oluşturan ve şifreleme algoritmasının tersine çalışan algoritmadır [56]. Şekil 3.1'de simetrik şifreleme akış diyagramı verilmiştir.



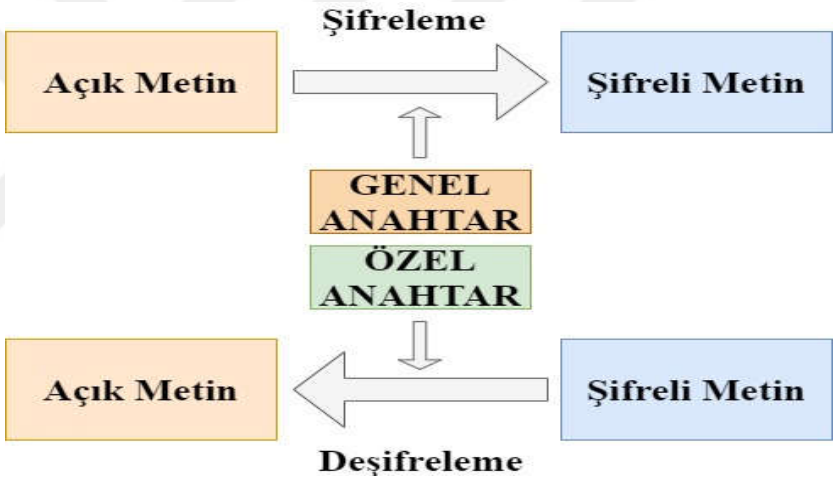
Şekil 3.1. Simetrik şifreleme akış diyagramı

3.1.2. Asimetrik şifreleme

Asimetrik şifrelemede şifreleme ve deşifreleme işlemleri için farklı anahtarlar kullanılır. Bu anahtarlardan birine açık anahtar diğerine ise özel anahtar denir. Kullanılacak olan bu iki anahtar birlikte üretilirler ve bu anahtarların arasında mantıksal bir bağ vardır. Asimetrik şifrelemede şifreleme işlemi herkes tarafından bilinen açık anahtarla yapılarak

şifreli bilgi gönderilebilir. Şifreli bilgi sadece şifrelemede kullanılan açık anahtarın karşılığı olan özel anahtar ile açılabilir. Şifreleme ve deşifreleme işlemi birbirinin simetriği olmayan algoritmalarla gerçekleştiğinden dolayı bu sistem asimetrik şifreleme sistemi olarak bilinir [13].

Asimetrik şifreleme sistemlerinde açık anahtar herkesin erişimine açıktır, özel anahtar ise sadece şifreli bilgiyi alacak kişinin erişebileceği şekilde saklanmalıdır. Böylelikle bu sistemde iletişim içerisindeki tarafların aynı gizli bilgiyi tutma durumları ortadan kalkmıştır. Asimetrik şifreleme sistemlerinin iki temel kullanım yeri vardır. Bunlar sayısal imza ve şifreleme uygulamalarıdır [57]. Asimetrik şifreleme algoritmalarına RSA, El Gamal ve Diffie-Hellman algoritmaları örnek olarak verilebilir. Şekil 3.2'de asimetrik şifreleme akış diyagramı verilmiştir.



Şekil 3.2. Asimetrik şifreleme akış diyagramı

3.1.3. Kaos tabanlı şifreleme

Birçok disiplinlerarası uygulamada kullanılabilen kaos teorisinin kriptoloji bilimiyle de doğal bir ilişkisi bulunmaktadır. Bu ilişki Shannon'un [53] belirtmiş olduğu "herhangi bir şifreleme sisteminin güvenilir olması için sahip olması gereken karıştırma ve yayılma" özelliklerinin kaotik sistemlerin başlangıç şartlarına karşı hassasiyet göstermesi, doğrusallık göstermemesi ve zengin dinamik davranışlar göstermesi özellikleriyle örtüşmesi sonucuyla sağlanabilmektedir.

Kaotik sistemler karıştırma ve yayılma özelliklerini gösteren sistemlerdir. Kaotik sistemlerin başlangıç şartlarına ve sistem parametrelerine bağımlılığı, bir kaotik

sistemden üretilen değerler kümesi boyunca yayılma özelliğini sağlar. Başlangıç şartları ve sistem parametrelerindeki çok küçük bir değişiklikle farklı değerler kümesi oluşacağından bu bağımlılığın derecesi çok güçlüdür. Bu sebeple kaotik sistemlerin başlangıç şartları ve sistem parametrelerine bağımlılığı kriptoloji uygulamalarında kullanılan sistemlerin yayılma gereksinimini karşılayacak seviyededir [58].

Kaotik bir sistemden üretilen tüm değerlerin bir kısmı ile istatistiksel olarak başlangıç şartları ve sistem parametrelerinin tam değerlerine ulaşılması imkânsızdır. Ergodiklik olarak tanımlanan bu özellikleri sebebiyle kaotik sistemler şifreleme uygulamalarında kullanılan sistemlerin karıştırma gereksinimini de sağlamaktadır [59].

Bu tez çalışması kapsamında tasarlanan kaos tabanlı şifreleme yöntemleri, simetrik şifreleme kuralları baz alınarak oluşturulmuştur.

3.2. Rastgele Sayı Üreteci (RSÜ)

Rastgele sayılar tahmin edilmesi zor veya değerinin ne olacağının bilinme olasılığı yok denecek kadar az olan sayılardır. Rastgele sayı üreteçleri çıkışında rastgele sayılar oluşturan sistemlerdir. Rastgele sayı üreteçlerinde üretilen sayılar bir önce ve bir sonraki üretilen sayılarla hiçbir şekilde istatistiksel olarak bir ilişkiye sahip değildirler. Rastgele sayılar, bu gibi özelliklerden dolayı rastgele süreçlerin modellerinin oluşturulması, sayısal analiz yöntemleri ve Monte Carlo metodu uygulamaları gibi bilgisayar uygulamalarında kullanılır. Bu uygulamaların dışında iletişimde iletilen bilgi içeriklerinin şifrelenmesinde de rastgele sayılar sıklıkla kullanılmaktadır [60].

3.2.1. RSÜ çeşitleri

Rastgele sayı üreteçleri, sözde rastgele sayı üreteci (SRSÜ) ve gerçek rastgele sayı üreteci (GRSÜ) olarak iki türe ayrılmıştır.

3.2.1.1. Sözde rastgele sayı üreteci (SRSÜ)

Sözde rastgele sayı üreteçleri belirli bir algoritma ile oluşturulan deterministik sayı dizilerinden oluşan sistemlerdir. Tohum denilen başlangıç durumundan bir dizi çıkış üretilir. Çıkışın tamamıyla tohum verisinin bir fonksiyonu olmasından dolayı çıkışın

gerçek entropisi tohumun entropisini asla geçemez. SRSÜ, seçilen bir tohum değeri ile çıkışında rastgele sayı üretme işlemi yaptığından dolayı seçilen tohum değerinin de rastgele olması gerekir [61].

Üretilen sözde rastgele dizilerin gerçek rastgele dizilerden mümkün olduğunca ayırt edilememeleri gerekmektedir. Örneğin bu diziler sıkıştırılamaz olmalıdırlar. Bu ve benzeri özellikler NIST 800-22 testi gibi testler ile deneysel olarak ölçülebilir.

Pek çok uygulama için sözde rastgele üreteçleri oldukça verimlidir. Kriptografik uygulamalar için de kimse tarafından tahmin edilemeyecek sözde rastgele bitlerin kullanılması önemli bir husustur. Kriptografik uygulamalardan iyi bir sonuç alınabilmesi durumu rastgele sayı üreteçlerinin özelliklerine aşırı derecede bağlıdır. Bir rastgele sayının tahmin edilememesi veya bilinememesi kriptografik çalışmaların temelini oluşturan etmenlerdendir. Kriptografi uygulamalarında kullanılacak bir SRSÜ tahmin edilemez olmalıdır. Yani, rastgele sayı dizisini oluşturan algoritmaya ilişkin tüm bilgi ve akıştaki tüm önceki bit değerleri verilse bile bir sonraki rastgele bitin ne olacağını tahmin etmek matematiksel olarak çok zor olmalıdır.

3.2.1.2. Gerçek rastgele sayı üreteci (GRSÜ)

Gerçek rastgele sayı üreteçleri girişleri doğal proseslerin rastgeleliğini kullanan, deterministik olmayan bir algoritmayla rastgele sayı üreten sistemlerdir. GRSÜ, donanım ve yazılım tabanlı olarak iki teknikle gerçeklenebilir [60].

Donanım tabanlı gerçek rastgele sayı üreteçleri, donanımsal bir ortamda oluşan gürültü işaretlerinin alınmasını temel alarak rastgele sayı üreten üreteçlerdir. Buna, üzerinden akım geçen bir direncin ısıl gürültüsü, bir osilatör devresinin faz gürültüsü durumları örnek olarak verilebilir. Bu prosesler sonucu oluşan işaretler de kendi aralarında ilişkili olabileceğinden dolayı tam olarak rastgeleliği sağlamak için çıkış değerleri basit bir algoritmayla yeniden bir işlem geçirebilir [62].

Yazılım tabanlı gerçek rastgele sayı üreteçleri sistemin saati, sabit diske erişim gibi bilgisayar tabanlı işlemleri temel alır. Yazılım tabanlı gerçek rastgele sayı üreteçlerini gerçeklemek, donanım tabanlı olanlara nazaran daha zordur.

Gürültü ortamlarına entropi kaynağı adı verilir. Entropi kaynağı, alınan sayıların üretiminin tekrarlanmaması ve tahmin edilemez olması açısından önemlidir. Ek bir işlem olarak entropi kaynaklarından alınan değerlerin rastgeleliğinin kuvvetlendirilmesi ve sayılar arasındaki ilişkinin ortadan kaldırılması için süreç sonrası işlemi uygulanmaktadır. Bu tamamen deterministik bir yöntemdir. Entropi kaynağından elde edilen rastgele sayılar giriş olarak kullanılır ve çıkışta, girişten daha kısa bit değerleri elde edilir.

3.2.2. Rastgele sayı üreteçlerine uygulanan NIST testleri

Rastgele sayı üreteçlerinin ürettiği sayı dizilerinin rastgeleliğini ölçmek için bazı istatistiksel testler kullanılır. Teste tabi tutulan sayı dizilerinin rastgele olduğu bu testlerin hepsinden başarılı olarak geçtiğinde kabul edilir [63]. Literatürde en sık kullanılan rastgelelik testleri NIST 800-22 ve FIPS 140-2 testleridir [64]. Tez çalışması için yapılan rastgelelik test çalışmalarında NIST 800-22 testi kullanılmıştır.

NIST 800-22 testinde en az 1 milyon adet veri ile rastgelelik testinin yapılması önerilmektedir. NIST 800-22 testi 15 ayrı testten oluşan bir yapıdadır. NIST 800-22 testinin her bir alt testinde bir p (probability) değeri hesaplanır. Testlerin başarılı olarak sonuç verebilmesi için her bir p değerinin 0.01'den büyük çıkması gerekmektedir [65]. Her bir test n uzunluktaki aynı bit dizisine uygulanır. Testlerin her birinin sonucunda testi geçen blok sayısı verilir ve p değeri hesaplanır. Teste girecek blok uzunluğu ve blok sayısı kullanıcı tarafından belirlenir. NIST 800-22 testinin içinde bulunan 15 alt testtin neler olduğu kısa açıklamalarıyla birlikte verilmiştir.

1. **Frekans testi:** Bit dizisindeki 1 ve 0 değerlerinin oranını inceler.
2. **Blok frekans testi:** m bitlik bit bloklarının 1 ve 0 oranını inceler.
3. **Akış testi:** Dizideki 1 ve 0 bloklarının sayısını inceler.
4. **Bir blok içerisinde en uzun birler akış testi:** Bu test üretilen bit dizisinde art arda gelen en uzun birlerin akış değeri üzerine çalışır. Dizi sabit bir sayıda bit kümesi halinde bloklara ayrılır. Bu blokların her biri için akış testi uygulanır ve çıkan sonuç değerleri eşik değeri ile karşılaştırılır.
5. **İki matris derece testi:** Sabit uzunluklu bit bloklarıyla her birinin bir satırı belirlemesi şekliyle bir matris oluşturulur ve bu matrisin derecesi hesaplanarak bloklar arasında doğrusal bir bağımlılık olup olmadığına bakılır.

6. **Ayrık Fourier dönüşüm testi:** Bu testte üretilen bit dizisinin ayrık Fourier dönüşümü alınarak dizinin periyodikliğinin incelenmesi gerçekleştirilir.
7. **Örtüşmeyen şablon eşleştirme testi:** Üretilen dizi içerisinde m bitlik bir bloğun tekrarını inceler. Tekrarın oluşması durumunda, tekrarın olduğu bloktan itibaren yeni bir m bitlik blok oluşturulur.
8. **Örtüşen şablon eşleştirme testi:** Üretilen dizi içerisinde m bitlik bir bloğun tekrarını inceler. Tekrarın oluşması durumunda blok 1 bit ötelenerek yeni bir blok oluşturulur.
9. **Maurer'in "evrensel istatistik" testi:** Bu test bit dizisinin veri kaybı olmadan ne kadar sıkıştırılabileceğini inceler.
10. **Doğrusal karmaşıklık testi:** Dizinin karmaşıklığını kontrol eden testtir.
11. **Seri testi:** Tekrar eden m bitlik 2^m tane bloğun tekrarlanma sayısının dağılımını inceleyen testtir.
12. **Yaklaşık entropi testi:** Bu test, m bitlik örtüşen olası örneklerin frekansını komşu uzunluktaki bitler veya iki ardışık bit için hesaplar.
13. **Birikimli toplamlar testi:** Bu test üretilen diziyi bloklara ayırıp bu blokların 0 ve 1 denge oranını belirleyerek bloklar arasındaki dengesizlik farkına bakar.
14. **Rastgele gezinimler testi:** Üretilen bit dizisi ardışık uzunluklu bloklara ayrılıp, blokların 1 ve 0 dengesi belirlenir. Bunun sonrasında blokların dengesinin dağılımını inceler.
15. **Rastgele gezinimler değişken testi:** Üretilen bit dizisi ardışık uzunluklu bloklara ayrılıp, blokların 1 ve 0 dengesi belirlenir. Sonrasında test ortalama değerden sapma miktarını belirler.

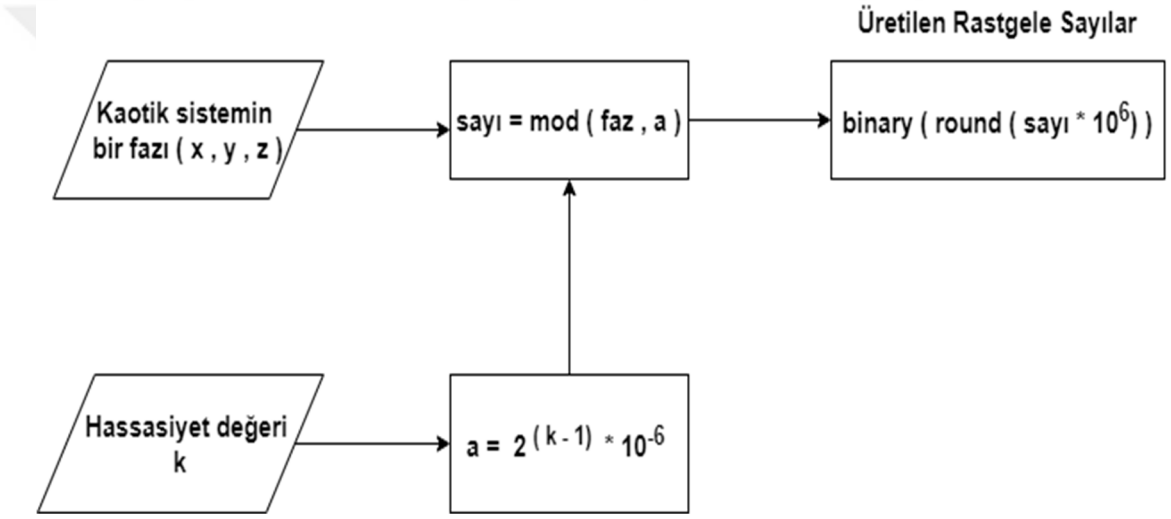
3.2.3. Kaos tabanlı RSÜ tasarımları

Kaotik sistemlerin ürettikleri işaretler (sayı dizileri) sayısal çözüm algoritmaları kullanılması sonucunda meydana gelir. Oluşturulan bu işaretler pozitif ve negatif desimal değerler olarak elde edilir. Elde edilen bu desimal değerler de rastgele sayı üreteçleriyle ikilik tabandaki sayı değerlerine dönüştürülür. Tez çalışmasında, ikilik tabanda elde edilen bu sayı değerleri şifreleme uygulamalarında kullanılan anahtarları oluşturmaktadır. İkilik tabanlı değerlerin elde edilebilmesi için 3 çeşit RSÜ tasarım çalışması yapılmıştır.

Önerilen RSÜ tasarım çalışmaları; mod alma, desimalden ikilik tabana dönüştürme ve kayan noktalı sayı yöntemleridir.

3.2.3.1. Mod alma yöntemi

Bu yöntemde kaotik sistemden üretilen değerler, belirlenen hassasiyet bit değeri sonucunda bulunan a parametresi ile mod işlemine girer. Bu işlemin sonrasında oluşan değerler gerekli çarpım (sayıyı 6 basamak ötelemek için) ve yuvarlama işlemlerinden sonra ikili değerlere dönüştürülür. Böylelikle rastgele sayı dizisi elde edilmiş olur. Mod alma yöntemi akış diyagramı Şekil 3.3'te gösterilmiştir.

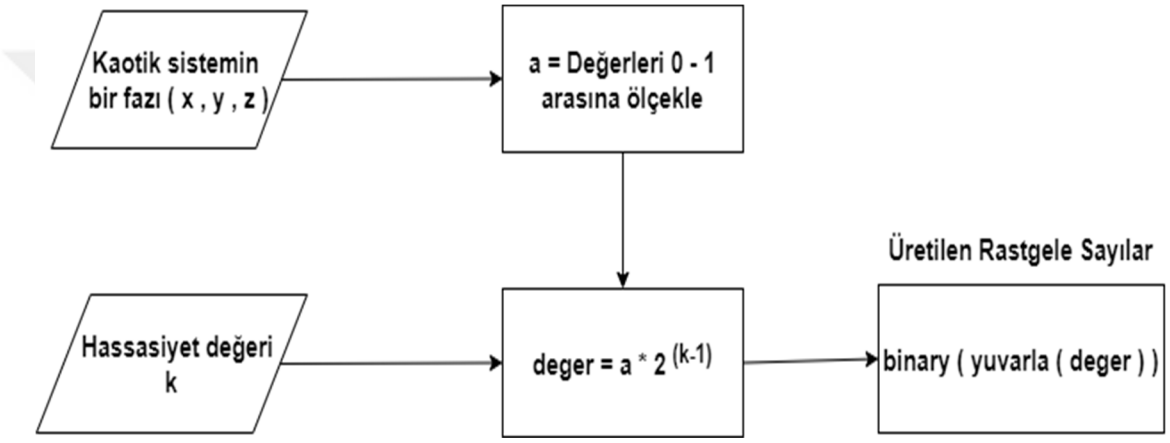


Şekil 3.3. Mod alma yöntemi akış diyagramı

Örnek olarak kaotik sistemden gelen veri setinin ilk değeri 3.82716 ve seçilen hassasiyet değeri de 8 bit olarak alınsın. İlk olarak 3.82716 değerinin, a parametresine göre mod işlemi gerçekleştirilir. a parametresi, $2^{8-1} * 10^{-6}$ işleminden 0.000255 olarak bulunur. Mod işlemini yapacak değerin 10^{-6} ile çarpılmasının nedeni kaotik sistemlerde ondalık değerlerin daha değişken olması ve rastgele sayı üretiminde de bu ondalık değerli kısımlardan yararlanılması içindir. mod(3.82716,0.000255) işleminin sonucu $12 * 10^{-5}$ değeri olarak elde edilir ve sonrasında $12 * 10^{-5} * 10^{6}$ işlemi yapılır. İşlemin sonucu olan 120 desimal değeri hassasiyet bit değeri 8 olarak seçilmesinden dolayı ikilik taban dönüşümü sonucunda "01111000" olarak elde edilir. İlk değerden sonraki veri seti değerleri de sırasıyla bu işlemlere tabi tutularak rastgele sayı dizisi elde edilmiş olunur.

3.2.3.2. Desimalden ikilik tabana dönüştürme yöntemi

Bu yöntem için öncelikle kaotik sistemden elde edilen negatif ve pozitif desimal değerlere sahip veri seti 0 ile 1 değerleri arasına $((X - X_{min})/(X_{max} - X_{min}))$ işlemiyle ölçeklenir. 0-1 arasında ölçeklenen veriler seçilen hassasiyet bit değerine göre çarpma işlemine tabi tutulur. Çıkan değerler gerekiyorsa yuvarlama işlemine girer ve en son olarak elde edilen tamsayı değerleri hassasiyet değeri olan bit sayısınca ikilik tabanlı sayıya dönüştürülür ve böylelikle rastgele sayı dizisi elde edilmiş olur. Desimalden ikilik tabana dönüştürme yöntemi akış diyagramı Şekil 3.4'te gösterilmiştir.



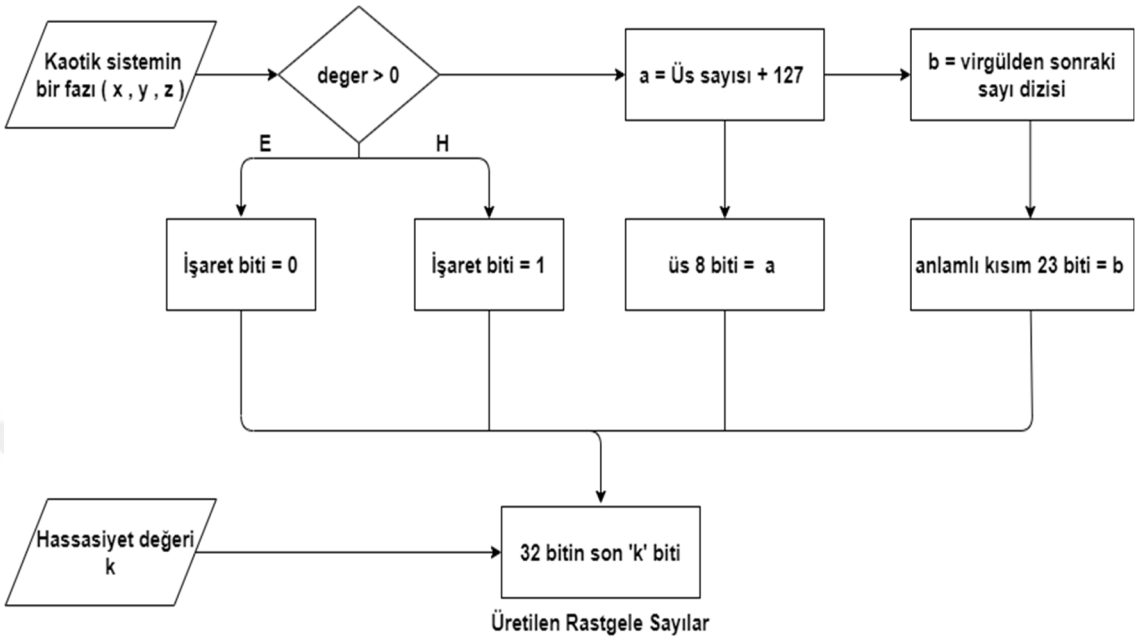
Şekil 3.4. Desimalden ikilik tabana dönüştürme yöntemi akış diyagramı

Örnek olarak kaotik sistemden gelen veri setinin; ilk değeri 2.3167, en yüksek değeri 11.2318, en düşük değeri ise -3.9162 ve seçilen hassasiyet değeri 12 bit olarak alınsın. Veri setinin en yüksek değeri 1 ve en düşük değeri 0 olacak şekilde ölçekleme işlemi yapıldıktan sonra ilk değer olan 2.3167 değeri, 0.4115 olarak hesaplanır. Seçilen hassasiyet değeri 12 bit olduğu için $0.4115 * 2^{12-1}$ işlemi gerçekleşir. İşlemin sonucunda desimal 1685 değeri elde edilir. 1685'in ikilik tabanda 12 bit olarak karşılığı "011010010101" şeklinde bulunur. İlk değerden sonraki veri seti değerleri de sırasıyla bu işlemlere tabi tutularak rastgele sayı dizisi elde edilmiş olunur.

3.2.3.3. Kayan noktalı sayı yöntemi

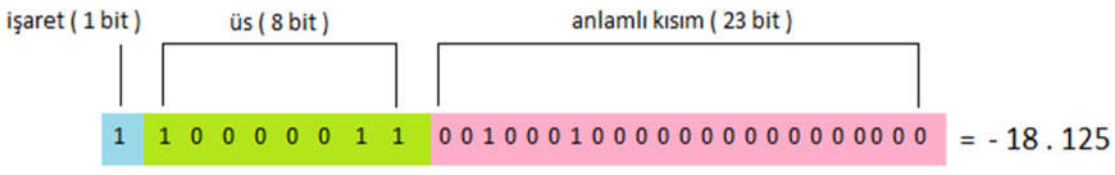
Rastgele sayı üretiminde kullanılan üçüncü yöntem tek duyarlı kayan noktalı sayıya dönüştürme yöntemidir. Bu yöntem IEEE 754 standardına göre düzenlenmiştir. Tek duyarlı gösterimde değer 32 bit ile ifade edilir. Bu bitlerden 1 tanesi işaret, 8 tanesi üs,

geriye kalan 23 tanesi de anlamlı kısmın gösterimi için kullanılır. Şekil 3.5'te Kayan noktalı sayı yöntemi akış diyagramı gösterilmiştir.



Şekil 3.5. Kayan noktalı sayı yöntemi akış diyagramı

Örnek olarak kaotik sistemin seçilen fazının ilk değeri -18.125 olarak alınsın. -18.125 sayısı, negatif bir sayı olduğu için işaret biti 1 olarak belirlenir. 18.125 sayısının ikilik tabanda karşılığı 10010.001'dir, daha sonra bu değer $1.0010001 * 10^4$ olarak üs sayısının hesaplanabileceği bir formda yazılır. Üs sayısı 4 olarak formülde yerine konur ve 4+127 işleminden elde edilen 131 sayısı ikilik tabana çevrilerek 8 bitlik üs kısım "10000011" olarak bulunmuş olur. Son 23 anlamlı kısım ise üs sayısı elde edildikten sonra virgülden itibaren gelen sayı dizisidir. 32 bit elde edildikten sonra kullanıcıdan girilen hassasiyet değeri ile 32 bit sayı dizisinin sondan kaç bitinin seçileceği belirlenir. İlk değerden sonraki faz değerleri de sırasıyla bu işleme tabi tutularak rastgele sayı dizisi elde edilmiş olunur. Şekil 3.6'da -18.125 sayısının IEEE 754 tek duyarlı kayan noktalı sayı yöntemi örnek gösterimi verilmiştir.



Şekil 3.6. Kayan noktalı sayı yöntemi örnek gösterimi

3.3. Güvenlik Analizleri

Bu tez çalışmasında çoklu ortam verilerinin XOR, Tur sayılı XOR, S-kutusu & XOR ve Tur sayılı S-kutusu yöntemleriyle şifrelenmesi sonucu şifreleme işlemlerinin başarılı ve güvenilir olup olmadığına dair sonuçlar veren bazı güvenlik analizleri kullanılmıştır. Bu analizler; histogram analizi, korelasyon analizleri, entropi analizi, NPCR ve UACI analizleri, PSNR analizi ve harf frekans analizleridir.

3.3.1. Histogram analizi

Histogram, veri değerlerinin içerdiği yoğunlukların dağılımını gösteren bir analiz grafiğidir. Şifreli verilerin çözülebilmesi için saldırgan histogram değerlerini kullanarak frekans analizi yapmaktadır. Bu gibi istatistiksel saldırılara karşı koymak için verilerin, belirli değerlerin ağırlıkta olduğu histogram grafiği yerine nerdeyse düz gibi homojen dağılımlı bir histogram grafiğine sahip olması gerekmektedir [66]. Böylelikle orijinal değerlerin histogramı ile şifreli değerlerin histogramı birbirinden farklı yapılarak bu tür saldırılar engellenebilir. Şifreli verinin histogramının homojen dağılımı iyi bir rastgeleliğin ve şifreleme algoritmasının kaliteli olduğunun bir göstergesidir. Bu çalışmada histogram analizi ses, görüntü ve video verilerinde kullanılmaktadır.

3.3.2. Korelasyon analizleri ve pearson korelasyon katsayıları

İki rastsal değişken arasındaki doğrusal ilişkinin yakınlığı korelasyon analizi ile belirlenir. n elemanlı bir dizide x ve y rastgele iki değişken olmak üzere pearson korelasyon katsayısı denklem 3.1 ile hesaplanabilir [53].

$$r = \frac{\sum_{i=1}^{n}(x_i - x_{ort}) * (y_i - y_{ort})}{\sqrt{\sum_{i=1}^{n}(x_i - x_{ort})^2 * (y_i - y_{ort})^2}} \tag{3.2}$$

Pearson korelasyon katsayısı, iki uç değer olan -1 ve +1 değerleri arasında sonuç verir. Katsayı değerinin bu uç değerlere çok yakın olması durumunda, analizin yapıldığı doğrultuda komşu veri değerlerinin arasında güçlü bir ilişki olduğundan bahsedilebilir. Katsayı değerinin 0'a yakın olması durumunda ise analizin yapıldığı doğrultuda komşu veri değerlerinin arasındaki ilişkinin zayıf olduğu söylenebilir.

Korelasyon analizlerinde oluşan grafiklerde ise grafik eğer doğrusal bir eksende sonuç verirse analizin yapıldığı doğrultuda bitişik komşu değerlerin birbiriyle uyumlu olduğu yani korelasyonun güçlü olduğu sonucuna varılır. Eğer grafikte homojen bir dağılım gerçekleştiyse korelasyonun zayıf olduğu sonucuna varılır.

Orijinal görüntü ve video verilerinde dikey, yatay ve diyagonal doğrultularda, orijinal ses verilerinde ise yatay doğrultuda komşu veri değerlerinin güçlü korelasyonları mevcuttur. İyi şifrelenmiş verilerde ise korelasyon sonuçları o doğrultularda homojen bir dağılım göstermelidir. Bu çalışmada korelasyon analizi ses, görüntü ve video verilerinde kullanılmaktadır.

3.3.3. Entropi analizi

Shannon tarafından kurulan bir matematik teorisi olan entropi bilgisi, sistemin içerdiği belirsizliğin derecesini ölçer [53]. Bu, bilginin ölçülebilir olduğunu da göstermektedir ve belirsizlik ile bilgi ters orantılıdır. Artan belirsizlik oranı, azalan tahmin yani azalan bilgi demektir. Çünkü sistemdeki belirsizlik, o sistemdeki bilgiye erişememe anlamına da gelmektedir. Entropi analizi denklem 3.2'de verilmiştir.

$$H(m) = \sum_{i=0}^{L-1} p(m_i) log_2(\frac{1}{p(m_i)}) \tag{3.2}$$

Denklem 3.2'de L, görüntü için piksel değerlerinin toplam sayısıdır. Bir pikselin m_i değerinde olma olasılığı $p(m_i)$ ile gösterilir ve $p(m_i)$ histogram değerlerini ifade eder. Eğer şifrelenmiş verinin entropisi logaritma L'ye yeterince yaklaşırsa verinin histogramı yeterince düzgün ve homojendir. Böylelikle belirsizlik en üst seviyededir denilebilir. Şifrelenmiş 3 kanallı bir görüntünün bir kanalının ideal entropi değeri 8'dir. Entropi değeri 8'e ne kadar yaklaşırsa belirsizlik durumu o kadar kuvvetli olur. Bu çalışmada entropi analizi görüntü ve video verilerinde kullanılmaktadır.

3.3.4. NPCR ve UACI analizleri

İki farklı görüntünün birbiriyle olan benzerlik ilişkisini karşılaştırmak önemli bir ölçektir. Görüntü şifreleme uygulamalarında benzerlik ilişkisini ölçmek için diferansiyel analiz yöntemleri kullanılır. Kerchoff'a göre iyi bir şifreleme için kullanılan gizli anahtarın

uyumsuzluğa karşı hassas olması gerekmektedir [67]. Çünkü gizli anahtardaki en ufak bir değişiklik şifrelenmiş görüntü üzerinde önemli farklılıklara neden olur. Bu hassasiyetin ölçüsü NPCR ve UACI olmak üzere iki diferansiyel analiz ile gerçekleştirilir. NPCR değiştirilen piksellerin sayısını, UACI ise değiştirilen piksellerin ortalama değerini verir [68]. Denklem 3.4 ile NPCR analizi ve denklem 3.5 ile UACI analizi hesaplanabilir.

$$Dif(i,j) = \begin{cases} 1\,, ise\ C_1(i,j) \neq C_2(i,j) \\ 0\,, ise\ C_1(i,j) = C_2(i,j) \end{cases} \tag{3.3}$$

$$NPCR = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} Dif(i,j) * 100\% \tag{3.4}$$

$$UACI = \frac{1}{MN}\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|C_1(i,j) - C_2(i,j)|}{255} * 100\% \tag{3.5}$$

Denklemlerde, M görüntünün toplam satır sayısını, N görüntünün toplam sütun sayısını, C_1 orijinal görüntünün piksel değerini ve C_2 ise şifreli görüntünün piksel değerini temsil eder. Yapılan çalışmalara göre, NPCR'ın %99,6'dan büyük, UACI'ın ise %30'a yakın ve büyük olması kaliteli bir şifreleme işlemi için eşik değerler olarak gösterilmiştir [69]. Bu çalışmada NPCR ve UACI analizleri görüntü ve video verilerinde kullanılmaktadır.

3.3.5. PSNR analizi

MSE, şifreli veri ile orijinal veri arasındaki değişimin değerini gösterir. Tez çalışması kapsamında orijinal ses verisi ve şifreli ses verisi 8 bitlik (0-255) değerlere dönüştürüldüğünden dolayı değişim için en yüksek değer 255^2 yani 65025'e eşit olur. Bundan dolayı MSE'nin sonuç değeri 65025'e ne kadar yakınsa orijinal veri ile şifreli veri arasındaki değişen veri sayısı o kadar fazladır. PSNR, verinin gürültü ve kalite seviyesini gösterir. PSNR değeri hesaplanırken MSE değerinden yararlanılır. PSNR sonuç değerinin 0'a yakın çıkması şifreleme algoritmasının kaliteli olduğunun bir göstergesidir. Denklem 3.6 ile MSE analizi ve denklem 3.7 ile PSNR analizi hesaplanabilir.

$$MSE(I, I_0) = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[I - I_0] \tag{3.6}$$

$$PSNR = 20log_{10}(\frac{255}{\sqrt{MSE(I, I_0)}}) \tag{3.7}$$

Denklem 3.6'da, M ses verisindeki toplam satır sayısını, N toplam kanal sayısını, I şifrelenecek sesin veri değerini, I_0 ise şifrelenmiş sesin veri değerini ifade etmektedir. Bu çalışmada PSNR analizi ses verilerinde kullanılmaktadır.

3.3.6. Harf frekans analizi

Harf frekans analizi mesajdaki karakter çeşitliliğini gösteren analizin sonucudur. Şifreli harf frekans analizinin düz ve homojen bir dağılım göstermesi beklenir. Şifreli mesajın frekans bandının geniş olması yani karakter çeşitliliğinin orijinal mesajdaki karakter çeşitliliğine göre artması şifreleme algoritmasının kaliteli olduğunun göstergesidir. Ayrıca harf frekans analizi, orijinal metindeki her karakterin şifreleme işleminden sonra hangi karakterlere dönüştüğünü de göstermektedir. Böylelikle orijinal metinde bulunan aynı karakterlerin farklı karakterlere şifrelenebildiği de bu analizle tespit edilir. Bu çalışmada harf frekans analizi metin verilerinde kullanılmaktadır.

BÖLÜM 4. ÇOKLU ORTAM VERİLERİ İÇİN KAOS TABANLI ŞİFRELEME ALGORİTMALARI

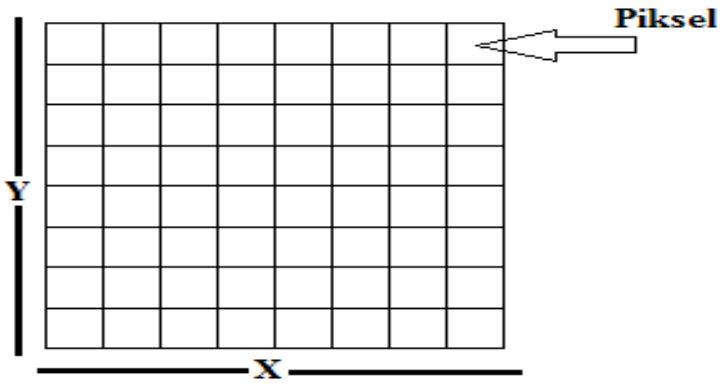
Bu çalışmada şifreleme ve deşifreleme uygulamalarında 4 çoklu ortam dosya türünün şifrelenebilmesi için 4 algoritma önerilmiştir. Şifrelenecek çoklu ortam verileri görüntü, metin, ses ve video verileridir. Bu dosya verilerinin şifrelenmesi için kullanılan yöntemlerin hepsinde S-kutuları ve XOR işlem yapısının tekil veya çoğul olarak kullanımı uygulanmıştır. Şifrelenmesi gerçekleştirilecek çoklu ortam verilerinin sayısal değerlerinin elde edilmesinin ve şifrelemede kullanılacak elemanların açıklamaları kısaca verilmiştir.

- **Görüntü dosyaları**

Sayısal görüntü a(x,y) gibi bir fonksiyonla ifade edilebilir. Bu fonksiyonda a parlaklık gibi bir şiddet birimini, x görüntünün enini, y ise görüntünün boyunu veren değerlerdir. Sayısal görüntü, enine ve boyuna sıralanmış piksellerden oluşan bir veri oluşumudur.

Piksel, görüntünün elde edilmesini sağlayan ve kontrol edilebilen en küçük birimdir. Görüntü ne kadar çok sayıda ve küçük piksellerden oluşmuşsa, görüntü o kadar kaliteli olmaktadır. Bir piksel kırmızı, yeşil ve mavi renklerin karışımından, bir görüntü ise piksellerin bir araya gelmesiyle oluşmaktadır. Çözünürlük ise bir defada ekranda görüntülenebilen piksel sayısıdır [70].

Uygulamada 3 kanallı (RGB) sayısal görüntüler kullanılmaktadır. Her bir kanal 8 bitlik (0-255) değerlerden oluşmaktadır. Görüntü dosyalarını oluşturan piksellerin gösterimi Şekil 4.1'de verilmiştir.



Şekil 4.1. Bir görüntüdeki piksellerin gösterimi

- **Metin dosyaları**

Metin içerisinde geçen karakterlerin değer dönüşümü ASCII tablosuna göre gerçekleşmektedir. Bu tablo dönüşümü sayesinde her bir karakter 8 bitlik bir değer ile ifade edilir. Örneğin "i" karakterinin ASCII kodunda desimal karşılığı 105, ikilik tabandaki karşılığı ise "01101001" şeklindedir. Tablo 4.1'de Metin şifreleme uygulamaları için kullanılacak karakterlerin ASCII kod değerleri verilmiştir.

Tablo 4.1. Metin şifreleme uygulamaları için kullanılacak karakterlerin ASCII kod değerleri

Kod	Char	Kod	Char	Kod	Char	Kod	Char	Kod	Char	Kod	Char
32	[space]	48	0	64	@	80	P	96	`	112	p
33	!	49	1	65	A	81	Q	97	a	113	q
34	ì	50	2	66	B	82	R	98	b	114	r
35	#	51	3	67	C	83	S	99	c	115	s
36	$	52	4	68	D	84	T	100	d	116	t
37	%	53	5	69	E	85	U	101	e	117	u
38	&	54	6	70	F	86	V	102	f	118	v
39	ë	55	7	71	G	87	W	103	g	119	w
40	(	56	8	72	H	88	X	104	h	120	x
41	)	57	9	73	I	89	Y	105	i	121	y
42	*	58	:	74	J	90	Z	106	j	122	z
43	+	59	;	75	K	91	[	107	k	123	{
44	,	60	<	76	L	92	\	108	l	124	|
45	-	61	=	77	M	93	]	109	m	125	}
46	.	62	>	78	N	94	^	110	n	126	~
47	/	63	?	79	O	95	_	111	o	127	

- **Ses dosyaları**

Ses, kulağın duyabileceği periyodik basınç titreşimleridir ve aynı zamanda örnekleme frekansına sahip bir veri dizisidir. Desibel (dB) ise ses seviyesini ölçmek için kullanılan birimdir. Bu tez kapsamında double veri yapısında -1 ile 1 arasında değerler alan ses dosyaları kullanılmıştır. -1 ile 1 arasındaki sayı değerlerini alan ses veri dizileri 8 bitlik ikili sayılara dönüştürülerek kullanılmaktadır. Uygulamalar için ilk olarak 1 kanallı veya 2 kanallı ses verisinden oluşan tüm sayı dizisi 1 ile toplanır ve böylelikle sayı dizisi 0 ile 2 arasına ölçeklenmiş olur. Sonrasında ses değerleri sırayla 2^{8-1} ile çarpılıp en yakın sayıya yuvarlandıktan sonra ikilik tabandaki değerlerine dönüştürülür. Yani en küçük değer olan -1 ses değerinin 8 bit karşılığı "00000000", desimal karşılığı ise 0'dır ve en büyük değer olan +1 ses değerinin 8 bit karşılığı "11111111", desimal karşılığı ise 255 olarak temsil edilir. Örnek olarak -0.213 ses verisi değerinin 8 bit karşılığı "01100100", desimal karşılığı ise 100 olarak bulunur.

- **Video dosyaları**

Video verileri görsel özellik açısından görüntü dosyalarıyla benzer özelliklere sahiplerdir. Videolar hareketsiz sayısal görüntülerin ardı sıra saniyede belirli bir sayıda (24, 30, 60) oynatılmasıyla oluşur. Bir saniyede oynatılan her bir görüntüye kare adı verilir. Sayısal bir videonun oluşması için bir ışık kaynağına, bir nesneye ve o nesnenin ışığı yansıtmasına ihtiyacı vardır. Belirtilen bu şartlar oluştuğunda ilk olarak görüntü ve ardından sayısal video oluşur [71]. Çalışmada video verilerinin tam veya kısmi şifrelenmesi işlemleri gerçekleştirilir. Videonun içeriğini oluşturan her bir kare 3 kanallıdır (RGB) ve her bir kanal da 8 bitlik (0-255) değerlerden oluşmaktadır.

- **S-kutusu**

S-kutuları doğrusal olmayan bir yapıda olup şifreleme algoritmalarında karıştırma işlemi yapan dolayısıyla algoritmaya gücünü veren elemanlardır. S-kutuları yer değiştirme kutuları olarak da adlandırılır ve simetrik blok şifreleme algoritmalarının en önemli elemanıdır. İyi bir S-kutusu seçimi şifrelemenin karmaşık ve başarılı olmasını direkt olarak etkiler. Şifreleme algoritmasının maruz kalabileceği doğrusal ve diferansiyel ataklara karşı şifreleme algoritmasını güvenli kılmak için kriptografik özellikleri iyi olan S-kutuları seçilmelidir [14]. Bu çalışmada S-kutularının kullanıldığı yöntemlerde

şifrelenecek olan veri S-kutularında karşılığı bulunan değerlerle yer değiştirme işlemine girmektedir.

- **XOR Kapısı**

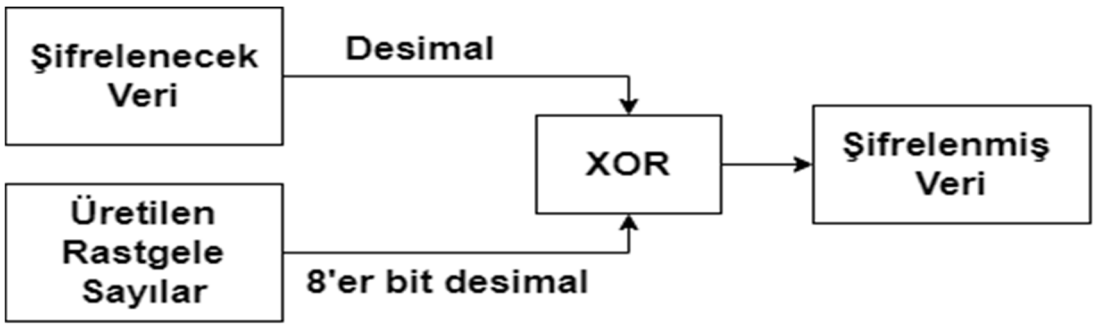
XOR kapısı, girişindeki işaretler birbirinden farklı olduğu zaman çıkış olarak 1, diğer tüm hallerde 0 çıkışı veren bir yapıdır. XOR kapısının boole cebiri eşitliği $A \text{ xor } B = A'B + AB'$ olarak ifade edilir. XOR işlemi şifreleme işlemlerinde kullanılan bir yöntemdir. Bu çalışmada XOR'un bulunduğu şifreleme yöntemlerinde ise rastgele sayılardan oluşan şifreleme anahtarı, şifrelenecek veriyle veya bir S-kutusu dönüşümüne uğramış veriyle XOR işlemine girer.

Bu çalışmada metin, görüntü, ses ve video verilerinin şifrelenebilmesi için kaos tabanlı 4 adet şifreleme yöntemi önerilmiştir. Bu yöntemler XOR, Tur sayılı XOR, S-kutusu & XOR ve Tur sayılı S-kutusu yöntemleridir.

4.1. XOR Yöntemi

Bu çalışmada önerilen ilk yöntem XOR ile şifreleme yöntemidir. Bu yöntemde şifrelenecek veri ile kaotik sistemden üretilen rastgele sayılar XOR işlemine tabi tutulur. Bu işlem için öncelikle kaotik sistemden elde edilen rastgele sayılar 8'er bitlik diziler haline getirilir ve sonrasında desimal değerlere dönüştürülür. Şifrelenmesi istenen çoklu ortam dosyalarından gelen veriler de desimal değerlere dönüştürülerek üretilen rastgele sayılarla XOR işlemine tabi tutulur. Böylelikle veri şifrelenmiş olur.

XOR ile şifreleme akış diyagramı Şekil 4.2'de gösterilmektedir. Şifreli veri, şifreleme algoritmasının tersine işlemler yapılarak deşifreleme işlemine tabi tutulur ve bu şekilde orijinal veri elde edilir.



Şekil 4.2. XOR yönteminin akış diyagramı

4.1.1. XOR yöntemi ile metin şifreleme

Örnek olarak kaotik sistemden elde edilen ilk 8 rastgele sayı "01001110" ve metnin ilk karakteri de "t" olarak alınsın. 8 bitlik ilk rastgele sayı dizisinin desimal karşılığı 78 olarak hesaplanır. İlk karakter olan "t" karakterinin ASCII tablosundaki desimal karşılığı 116'dır. 78 ve 116 değerleri XOR işlemine girdikten sonra sonuç değeri 58 olarak bulunur. 58 değerinin ASCII tablosundaki karşılığı ":" karakteridir. Sonuç olarak "t" karakteri, ":" karakterine dönüştürülerek şifrelenmiş olur.

4.1.2. XOR yöntemi ile görüntü şifreleme

Örnek olarak kaotik sistemden elde edilen ilk 8 rastgele sayı "11011010" ve görüntünün ilk kanalındaki ilk piksel değeri 201 olarak alınsın. 8 bitlik ilk rastgele sayı dizisinin desimal karşılığı 218 olarak hesaplanır. 201 ve 218 değerleri XOR işlemine girer ve sonuç değeri 19 olarak bulunur. Sonuç olarak ilk piksel 201 değerinden 19 değerine dönüştürülerek şifrelenmiş olur.

4.1.3. XOR yöntemi ile ses şifreleme

Örnek olarak kaotik sistemden elde edilen ilk 8 rastgele sayı "00101111" ve sesin ilk kanalındaki ilk değer 0.1391 olarak alınsın. İlk verinin ikilik tabandaki karşılığı "10010001" olarak bulunur. Bu iki 8'er bitlik diziler XOR işlemine girer. XOR işlemi ikilik tabanlı değer olarak "10111110" ve bu değerin desimal karşılığı da 190 olarak bulunur. Desimal 190 değerinin ses verisindeki karşılığı 0.4844 olarak hesaplanır. Sonuç olarak 0.1391 ses değeri, 0.4844 değerine dönüştürülerek şifrelenmiş olur.

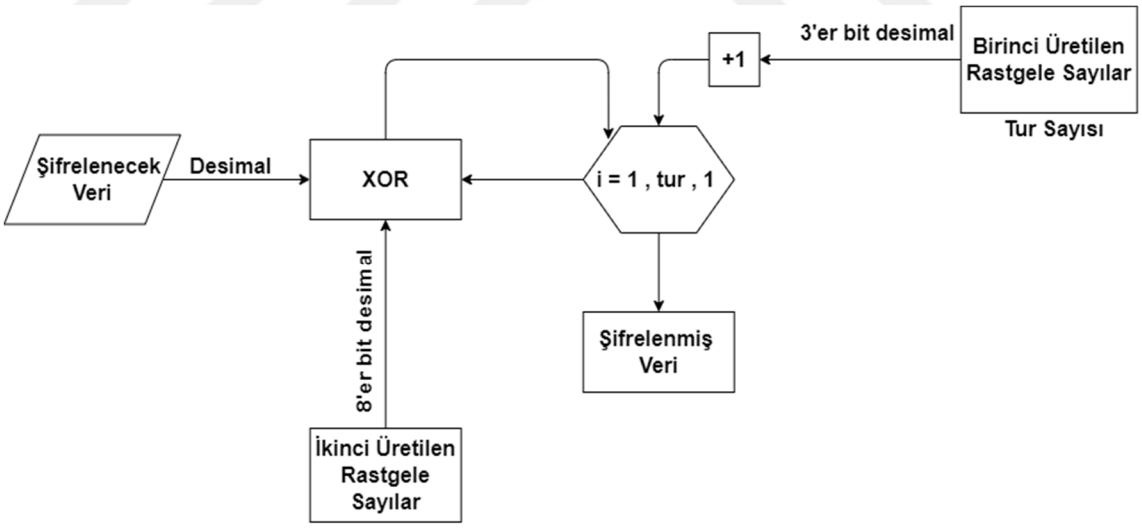
4.1.4. XOR yöntemi ile video şifreleme

Örnek olarak kaotik sistemden elde edilen ilk 8 rastgele sayı "01111001" ve videonun şifrelenecek karesinin ilk kanalının ilk piksel değeri 197 olarak alınsın. 8 bitlik rastgele sayının desimal karşılığı 121 olarak hesaplanır. 121 ve 197 değerleri XOR işlemine girdikten sonra sonuç değeri 188 olarak bulunur. Sonuç olarak 197 piksel değeri, 188 değerine dönüştürülerek şifrelenmiş olur.

4.2. Tur sayılı XOR Yöntemi

Bu şifreleme yöntemi 2 aşamadan oluşur. İlk olarak her bir verinin kaç farklı XOR işlemine tabi tutulacağının öğrenilmesi amacıyla tur sayısı belirlenir. İkinci olarak tur sayıları belirlendikten sonra XOR işlemi yapılır. Tur sayılarının belirlenmesinde ve XOR işleminde kullanılacak değerler için iki adet rastgele sayı dizisi kullanılır. Bu rastgele sayı dizileri kaotik sistemin seçilen faz değerlerinden üretilir. Üretilen rastgele sayı dizilerinden ilki tur sayısının belirlenmesi için 3'er bitlik diziler haline dönüştürülür. Bu 3'er bitlik diziler desimal değerlere dönüştürülür ve +1 değeri eklenerek her veri için tur sayısı en düşük 1 ve en yüksek 8 olacak şekilde belirlenmiş olur. Tur sayıları belirlendikten sonra ikinci rastgele sayı üretecinden gelen 8'er bitlik değerlerle XOR işlemleri yapılır. Bu işlemlerin sonunda veriler, tur sayısı kadar farklı rastgele sayılarla XOR işlemine girerek şifrelenmiş olur.

Tur sayılı XOR ile şifreleme akış diyagramı Şekil 4.3'te gösterilmektedir. Şifreli veri, şifreleme algoritmasının tersine işlemler yapılarak deşifreleme işlemine tabi tutulur ve bu şekilde orijinal veri elde edilir.



Şekil 4.3. Tur sayılı XOR yönteminin akış diyagramı

4.2.1. Tur sayılı XOR yöntemi ile metin şifreleme

Şifreleme, iki adımdan oluştuğu için kaos tabanlı iki adet rastgele sayı dizisi elde edilir. Örnek olarak ilk adımda şifrelenecek metnin ilk iki karakterinin tur sayılarını hesaplamak için üretilen ilk rastgele sayı dizisinin ilk 6 biti "001101" olarak alınsın. Bu dizi 3'er bitlik

diziler haline getirilir ve sonrasında desimal değerlere dönüştürülür. Dizilerin desimal karşılığı ilk üç bit için 1, ikinci üç bit için ise 5 olarak hesaplanır. Bu sayılara +1 değeri eklenerek ilk 2 karakterin tur sayıları sırasıyla 2 ve 6 olarak belirlenmiş olur. Şifrelemenin ikinci adımında ise üretilen ikinci rastgele sayı dizisi 8'er bitlik hale getirildikten sonra ilk 64 bitin desimal karşılıkları 121, 64, 14, 61, 184, 3, 90, 251 olarak alınsın. Metnin ilk karakteri de "t" olarak alınsın. "t" karakterinin ASCII kod karşılığı 116'dır. İlk karakter için tur sayısının 2 olarak bulunmasından dolayı 116 desimal değeri, ikinci sayı dizisinden elde edilen ilk iki desimal değer olan 121 ve 64 ile sırasıyla olacak şekilde XOR işlemlerine girer. 116 XOR 121 XOR 64 İşlemlerinin sonucu 77 olarak hesaplanır. 77'nin ASCII kod karşılığı "M" karakteridir. Bu şifreleme sonucu "t" karakteri, "M" karakterine dönüşerek şifrelenmiş olur. Metnin şifrelenecek ikinci karakter de "e" olarak alınsın. "e" karakterinin ASCII kod karşılığı 101'dir. Bu değer ikinci karakter için tur sayısı 6 olarak bulunmasından dolayı sırasıyla 14, 61, 184, 3, 90 ve 251 değerleriyle XOR işlemlerine girer ve 101 XOR 14 XOR 61 XOR 184 XOR 3 XOR 90 XOR 251 işlemlerinin sonucunda desimal 76 değeri elde edilir. 76'nın ASCII kod karşılığı "L" karakteridir ve sonuç olarak "e" karakteri, "L" karakterine dönüşerek şifrelenmiş olur.

4.2.2. Tur sayılı XOR yöntemi ile görüntü şifreleme

Örnek olarak, görüntünün şifrelenecek ilk iki pikselinin tur sayılarını hesaplamak için üretilen ilk rastgele sayı dizisinde, ilk 6 bit "010100" olarak alınsın. Bu dizi 3'er bitlik diziler haline getirilir ve sonrasında desimal değerlere dönüştürülerek ilk üç bit için 2, ikinci üç bit için ise 4 şeklinde hesaplanır. Bu sayılara +1 değeri eklenerek ilk iki pikselin tur sayıları 3 ve 5 olarak belirlenmiş olur. İkinci rastgele sayı dizisi 8'er bitlik hale getirildikten sonra ilk 64 bitin desimal karşılıkları 97, 10, 53, 109, 247, 6, 44, 1 olarak alınsın. Görüntünün ilk iki piksel değeri de 105 ve 106 olarak alınsın. İlk piksel değeri olan 105, tur sayısından dolayı ikinci sayı dizisinin ilk üç desimal değeri olan 97, 10 ve 53 sayıları ile sırasıyla XOR işlemlerine girer. 105 XOR 97 XOR 10 XOR 53 İşlemlerinin sonucu 55 olarak hesaplanır. Bu şifreleme işlemi sonucunda 105 piksel değeri 55 değerine dönüşerek şifrelenmiş olur. İkinci piksel olan 106 değeri, tur sayısı 5 bulunmasından dolayı sırasıyla 109, 247, 6, 44 ve 1 değerleriyle XOR işlemlerine girer ve 106 XOR 109 XOR 247 XOR 6 XOR 44 XOR 1 işlemlerinin sonucu 219 olarak bulunur. Böylelikle 106 piksel değeri 219 değerine dönüşerek şifrelenmiş olur.

4.2.3. Tur sayılı XOR yöntemi ile ses şifreleme

Örnek olarak ses verisinin şifrelenecek ilk 2 verisinin tur sayısını hesaplamak için üretilen ilk rastgele sayı dizisinde, ilk 6 bit "101010" olarak alınsın. Bu dizi 3'er bitlik diziler haline getirilir ve sonrasında desimal değerlere dönüştürülerek ilk üç bit için 5, ikinci üç bit için ise 2 şeklinde hesaplanır. Bu sayılara +1 değeri eklenerek ilk 2 verinin tur sayıları 6 ve 3 olarak belirlenmiş olur. İkinci rastgele sayı dizisi 8'er bitlik hale getirildikten sonra ilk 72 bitin desimal karşılıkları 78, 51, 114, 9, 23, 208, 132, 5 ve 76 olarak alınsın. Ses verisinin ilk kanalının ilk iki ses verisi de 0.14 ile -0.67 olarak alınsın. İlk veri değeri olan 0.14, 129 desimal değeri olarak hesaplanır ve bu değer, çıkan tur sayısından dolayı ikinci sayı dizisinin ilk 6 desimal değeri olan 78, 51, 114, 9, 23 ve 208 sayıları ile sırasıyla XOR işlemlerine girer. 129 XOR 78 XOR 51 XOR 114 XOR 9 XOR 23 XOR 208 işlemlerinin sonucu 64 olarak hesaplanır ve bu değerin ses verisine dönüşümü -0.5 olarak hesaplanır. Bu şifreleme işlemi sonucunda 0.14 değeri -0.5 değerine dönüşerek şifrelenmiş olur. İkinci veri değeri olan -0.67, desimal 42 olarak hesaplanır ve bu değer, tur sayısının 3 bulunmasından dolayı sırasıyla 132, 5 ve 76 değerleriyle XOR işlemlerine girer. 42 XOR 132 XOR 5 XOR 76 İşlemlerinin sonucunda 231 değeri elde edilir. Desimal 231 değerinin ses verisine dönüşümü 0.8047 olarak hesaplanır. Böylelikle -0.67 değeri 0.8047 değerine şifrelenmiş olur.

4.2.4. Tur sayılı XOR yöntemi ile video şifreleme

Örnek olarak videonun şifrelenecek karesinin ilk kanalının ilk iki pikselinin tur sayısını hesaplamak için üretilen ilk rastgele sayı dizisinde, ilk 6 bit "000101" olarak alınsın. Bu dizi 3'er bitlik diziler haline getirilir ve sonrasında desimal değere dönüştürülerek ilk üç bit için 0, ikinci üç bit için ise 5 şeklinde hesaplanır. Bu sayılara +1 değeri eklenerek ilk 2 pikselin tur sayıları 1 ve 6 olarak belirlenmiş olur. İkinci rastgele sayı dizisi 8'er bitlik hale getirildikten sonra ilk 56 bitin desimal karşılıkları 182, 64, 93, 204, 251, 17 ve 1 olarak alınsın. Şifrelenmesi istenen video karesinin ilk iki pikseli de 55 ve 40 olarak alınsın. İlk piksel değeri, tur sayısından dolayı ikinci sayı dizisinin ilk desimal değeri olan 182 ile XOR işlemine girer ve işlemin sonucunda 129 değeri elde edilir. Bu şifreleme işlemi sonucunda 55 piksel değeri 129 değerine dönüşerek şifrelenmiş olur. İkinci piksel değeri, tur sayısının 6 bulunmasından dolayı sırayla 64, 93, 204, 251, 17 ve 1 değerleriyle

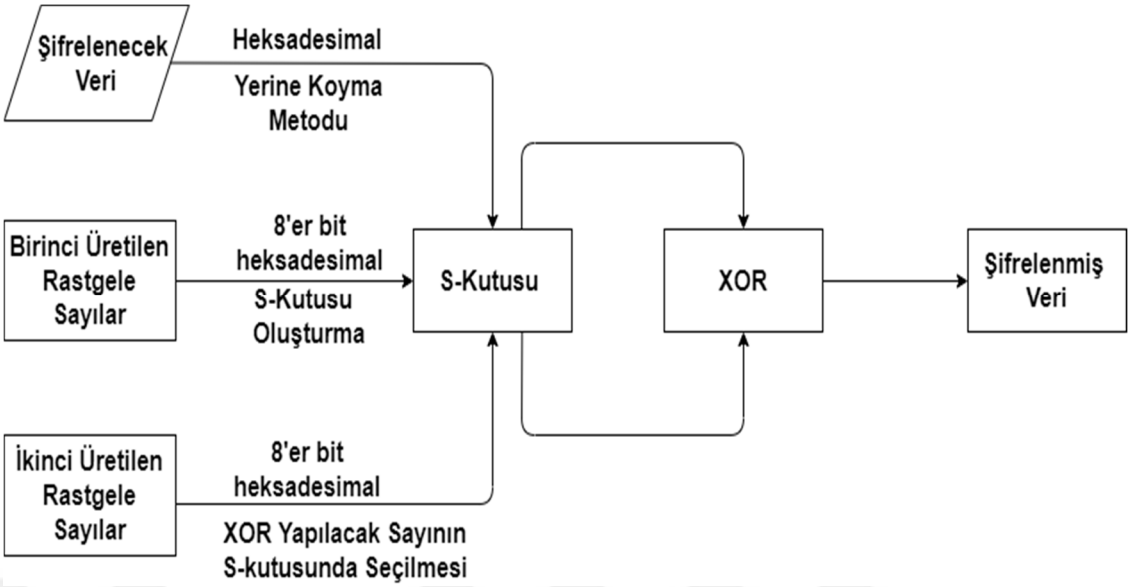
XOR işlemlerine girer ve 40 XOR 64 XOR 93 XOR 204 XOR 251 XOR 17 XOR 1 işlemlerinin sonucu 18 olarak bulunur. Böylelikle 40 piksel değeri 18 değerine dönüşerek şifrelenmiş olur.

4.3. S-kutusu & XOR Yötemi

Yöntem iki adımdan oluşmaktadır ve bu yöntem için kaotik sistemden iki adet rastgele sayı dizisi üretilir. İlk adım birinci rastgele sayı üretecinden 16 x 16'lık heksadesimal değerlerden oluşan S-kutusunun oluşturulması ve sonrasında verilerin heksadesimal değerlerinin S-kutusunda yerine konmasıdır. İkinci adım da ise ilk adım sonucu yerine koyma işleminden elde edilen değerlerle ikinci rastgele sayı üretecinden gelen değerlerin S-kutusunda yerine koyma işleminden sonra elde edilen değerleriyle XOR işlemi gerçekleştirilmesidir.

16 x 16'lık S-kutusunda 256 sayı olacağı için 8 x 256 bit rastgele sayı gereklidir. Bunun için seçilen kaotik sistemin belirlenen fazından 8 x 256 adetlik rastgele sayı dizisi üretilir. Bu sayılar 8'er bitlik hale getirildikten sonra desimal değerlere dönüştürülür. Desimal değerlere dönüştürülen sayılar mod alma işlemine tabi tutulurlar. Mod işlemi sonucunda desimal olarak 0 ile 255 değerleri arasında 256 farklı sayı elde edilir ve bu değerler 2 basamaklı heksadesimal değerlere dönüştürülerek 16 satır ve 16 sütunluk bir S-kutusu elde edilmiş olunur. S-kutusu oluşturulduktan sonra şifrelenecek verinin iki basamaklı heksadesimal değeri birinci basamağı S-kutusunda satır, ikinci basamak değeri S-kutusunda sütun olacak şekilde ayarlanır. Bu işlem sonucunda S-kutusunda bulunan sayı, verideki sayı yerine geçer ve şifrelemenin ilk adımı gerçekleşmiş olur. Şifrelemenin ikinci adımında, kaotik sistemden üretilen ikinci rastgele sayı dizisi kullanılır. Bu sayı dizisi ilk olarak 8'er bitlik diziler hale dönüştürülür. Sonrasında her bir 8 bitlik dizi iki basamaklı heksadesimal değerlere dönüştürülür. Elde edilen bu 2 basamaklı heksadesimal değerler S-kutusunda yerine koyma işlemine girer ve bu işlemin sonunda elde edilen değer ile şifrelemenin ilk adımının sonucunda elde edilen değer XOR işlemine girerek şifreleme tamamlanmış olur.

S-kutusu & XOR ile şifreleme akış diyagramı Şekil 4.4'te gösterilmektedir. Şifreli veri, şifreleme algoritmasının tersine işlemler yapılarak deşifreleme işlemine tabi tutulur ve bu şekilde orijinal veri elde edilir.



Şekil 4.4. S-kutusu & XOR yönteminin akış diyagramı

Tablo 4.2'de verilen S-kutusu örneği, bölüm 4.3 ve bölüm 4.4'te örneklerle anlatılan şifreleme işlemlerinde referans alınan değerlerin bulunduğu S-kutusudur.

Tablo 4.2. Örnek bir 16 x 16'lık S-kutusu

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	E8	EB	EA	E1	CE	A7	65	F8	45	32	8A	O9	3C	88	16	E3
1	68	41	B5	8B	5C	C8	54	0F	13	6A	1A	O3	E7	83	A3	4E
2	BE	O4	7D	B2	20	59	44	A9	3A	57	DB	9C	97	O1	2F	6F
3	E0	8D	2A	D1	84	40	82	FE	AC	E2	O6	A8	ED	1C	5B	A5
4	FA	75	78	87	73	BB	CA	7E	93	6C	C7	AF	7A	C0	17	66
5	D8	7F	6E	7C	36	39	9F	1D	47	DF	B6	BD	0D	D5	0C	49
6	O2	76	E5	98	31	A1	43	5F	46	33	89	86	AE	53	64	1E
7	BF	D3	3D	FC	DE	8F	37	25	9D	95	B3	85	A6	D9	28	BC
8	1F	52	38	7B	B4	69	D7	42	F4	DA	C5	63	30	27	FD	AD
9	EF	9B	72	9E	71	C1	E9	3E	B7	A2	5A	DD	80	61	4C	74
A	6B	0E	FB	90	51	D4	10	5D	96	F2	EC	DC	34	2B	F6	0B
B	22	B8	AA	79	OO	3F	18	77	5E	8C	C6	4D	D2	FF	BA	67
C	99	92	4F	81	12	C4	58	O8	0A	21	B1	11	C2	24	8E	2C
D	AB	70	C3	91	1B	2D	29	O7	A4	15	F7	F3	55	D6	B9	CD
E	23	F0	4B	O5	94	14	3B	50	E4	A0	2E	56	19	26	EE	9A
F	60	4A	CB	35	62	F5	CF	F9	6D	B0	D0	E6	CC	F1	C9	48

4.3.1. S-kutusu & XOR yöntemi ile metin şifreleme

Örnek olarak metnin ilk karakteri "t" olarak alınsın. "t" karakterinin ASCII tablosundaki desimal karşılığı 116, heksadesimal karşılığı "74" olarak hesaplanır. Kaotik sistemden üretilen rastgele sayıların 2 basamaklı heksadesimal değerleriyle S-kutusu oluştuktan sonra 7. satır 4. sütundaki değer "DE" olarak bulunur. Şifrelemenin ilk adımında "t" karakteri yani "74" heksadesimal değeri "DE" değerine dönüştürülmüş olur. İkinci adım için ikinci rastgele sayı dizisinde üretilen ilk 8 bit "00010011" olarak alınsın. Bu değerin heksadesimal karşılığı "13" değeridir. S-kutusuna bakıldığında 1. satır 3. sütun "8B" değeri olarak bulunur. İlk adımın sonunda elde edilen "DE" değeri ile ikinci adımdan elde edilen "8B" değeri XOR işlemine tabi tutulur ve sonuç olarak heksadesimal "55" değeri elde edilir. Bu değer desimal olarak 85, karakter olarak ASCII kod dönüşümüyle "U" karakterine karşılık gelmektedir. Böylelikle "t" karakteri, "U" karakterine dönüştürülerek şifrelenmiş olur.

4.3.2. S-kutusu & XOR yöntemi ile görüntü şifreleme

Örnek olarak görüntünün ilk kanalının ilk pikselinin değeri 60 olarak alınsın. Desimal 60'ın heksadesimal karşılığı "3C" olarak hesaplanır. Kaotik sistemden üretilen rastgele sayıların 2 basamaklı heksadesimal değerleriyle S-kutusu oluştuktan sonra 3. satır C. sütundaki değer "ED" olarak bulunur. Böylelikle şifrelemenin ilk adımında "3C" piksel değeri "ED" değerine dönüştürülmüş olur. İkinci adım için ikinci rastgele sayı dizisinde üretilen ilk 8 bit "10010011" olarak alınsın. Bu değerin heksadesimal karşılığı "83" değeridir. S-kutusuna bakıldığında 8. satır 3. sütun "7B" değeri olarak bulunur. İlk adımın sonunda elde edilen "ED" ile ikinci adımdan elde edilen "7B" değeri XOR işlemine tabi tutulur ve sonuç olarak heksadesimal "96" değeri elde edilir. Bu değer desimal olarak 150 değerine karşılık gelir. Böylelikle piksel değeri 60 değerinden 150 değerine dönüştürülerek şifrelenmiş olur.

4.3.3. S-kutusu & XOR yöntemi ile ses şifreleme

Örnek olarak ses verisinin ilk kanalının ilk değeri 0 olarak alınsın. Ses verisinin 0 değerinin desimal karşılığı 128, heksadesimal karşılığı ise "80" olarak hesaplanır. Kaotik

sistemden üretilen rastgele sayıların 2 basamaklı heksadesimal değerleriyle S-kutusu oluştuktan sonra 8.satır 0.sütundaki değer "1F" olarak bulunur. Böylelikle şifrelemenin ilk adımında "80" değeri "1F" değerine dönüştürülmüş olur. İkinci adım için ikinci rastgele sayı dizisinde üretilen ilk 8 bit "01110010" olarak alınsın. Bu değerin heksadesimal karşılığı "72" değeridir. S-kutusuna bakıldığında 7.satır 2.sütun "3D" değeri olarak bulunur. İlk adımın sonunda elde edilen "1F" ile ikinci adımdan elde edilen "3D" değerleri XOR işlemine tabi tutulur ve sonuç olarak heksadesimal "22" değeri elde edilir. Bu değerin desimal dönüşümü 34 olarak elde edilir ve bu da ses verisinde -0.2656'ya karşılık gelir. Böylelikle ses verisinin ilk değeri olan 0 değeri -0.2656 değerine dönüştürülerek şifrelenmiş olur.

4.3.4. S-kutusu & XOR yöntemi ile video şifreleme

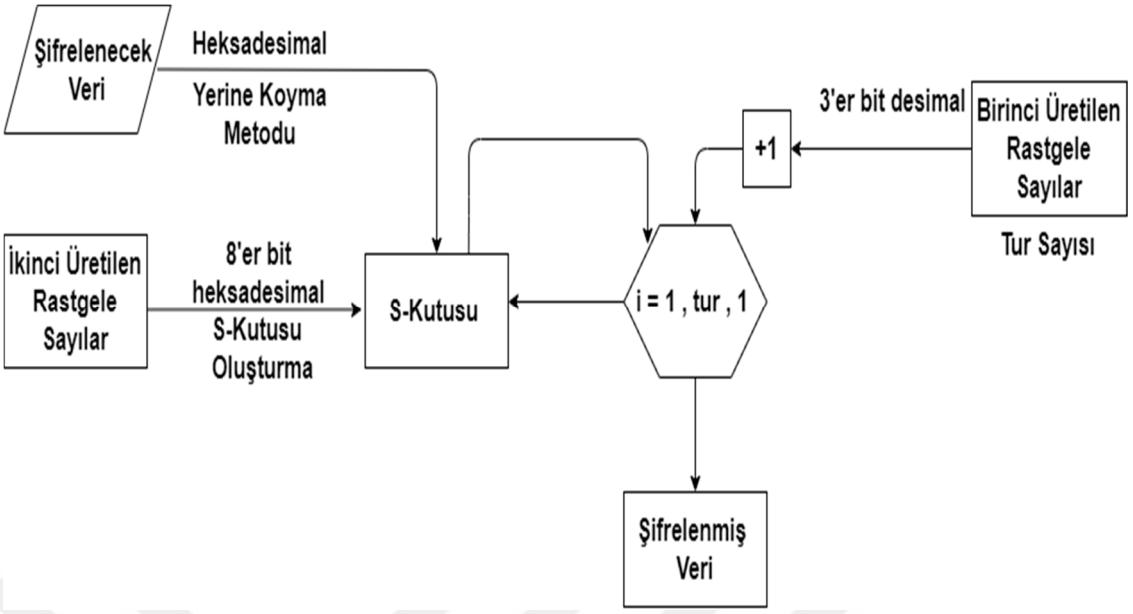
Örnek olarak videonun şifrelenecek karesinin ilk kanalının ilk pikseli 85 olarak alınsın. Desimal 85'in heksadesimal karşılığı "55" olarak hesaplanır. Kaotik sistemden üretilen rastgele sayıların 2 basamaklı heksadesimal değerleriyle S-kutusu oluştuktan sonra 5. satır 5. sütundaki değer "39" olarak bulunur. Böylelikle şifrelemenin ilk adımında heksadesimal "55" piksel değeri "39" değerine dönüştürülmüş olur. İkinci adım için ikinci rastgele sayı dizisinde üretilen ilk 8 bit "01110011" olarak alınsın. Bu değerin heksadesimal karşılığı "73" değeridir. S-kutusuna bakıldığında 7.satır 3.sütun "FC" değeri olarak bulunur. İlk adımın sonunda elde edilen heksadesimal "39" değeri ile ikinci adımdan elde edilen "FC" değeri XOR işlemine tabi tutulur ve sonuç olarak heksadesimal "C5" değeri elde edilir. Bu değer desimal olarak 197 değerine karşılık gelir. Böylelikle piksel değeri 85'ten 197 değerine dönüştürülerek şifrelenmiş olur.

4.4. Tur sayılı S-kutusu Yöntemi

Bu şifreleme yöntemi iki adımdan oluşmaktadır. İlk olarak her bir veri için S-kutusunda yerine koyma metodunun kaç tur uygulanacağının sayısı belirlenir. İkinci olarak tur sayıları belirlendikten sonra kaotik sistemden elde edilen rastgele sayılarla S-kutusunun oluşturulması ve oluşturulan S-kutusunda da yerine koyma işlemleri gerçekleştirilir.
Tur sayılarının belirlenmesinde ve S-kutusunun oluşturulması için iki adet rastgele sayı dizisi kullanılır. Bu rastgele sayı dizileri kaotik sistemin seçilen faz değerlerinden üretilir.

Üretilen rastgele sayı dizilerinden ilki tur sayısının belirlenmesi için 3'er bitlik diziler haline dönüştürülür. Bu 3'er bitlik diziler desimal değerlere dönüştürülür ve +1 değeri eklenerek her veri için kaç tur yerine koyma işlemi yapılacağı en düşük 1 ve en yüksek 8 olacak şekilde belirlenmiş olur. İkinci üretilen rastgele sayı dizisi ise 16 x 16'lık heksadesimal değerlerden oluşan S-kutusunun oluşturulmasında kullanılır. 16 x 16'lık S-kutusunda 256 sayı olacağı için 8 x 256 bit rastgele sayı gereklidir. Bunun için seçilen kaotik sistemin belirlenen fazından 8 x 256 adetlik rastgele sayı dizisi üretilir. Bu sayılar 8'er bitlik hale getirildikten sonra desimal değerlere dönüştürülür. Desimal değerlere dönüştürülen sayılar mod alma işlemine tabi tutulurlar. Mod işlemi sonucunda desimal olarak 0 ile 255 değerleri arasında 256 farklı sayı elde edilir ve bu değerler 2 basamaklı heksadesimal değerlere dönüştürülerek 16 satır ve 16 sütunluk bir S-kutusu elde edilmiş olunur. S-kutusu oluşturulduktan sonra şifrelenecek verinin heksadesimal değeri birinci basamağı S-kutusunda satır, ikinci basamak değeri S-kutusunda sütun olacak şekilde ayarlanır. Bu işlem sonucunda S-kutusunda bulunan sayı, verideki sayı yerine geçer. Böylelikle şifreleme işleminde ilk tur tamamlanmış olur. Bundan sonraki her yeni turun başlangıcında S-kutusundaki 2 basamaklı heksadesimal değerler "01" değeri azaltılarak her tur için farklı bir S-kutusu oluşturulmuş olunur (S-kutusunda o an olan "00" heksadesimal değeri her yeni turda "FF" değerine dönüşür). Bu işlemle S-kutusunda tekrardan 256 farklı heksadesimal değer oluşur ve böylelikle heksadesimal değerlerin yerlerinin değişmesinden dolayı her yeni turda S-kutusundan aynı değerlerin gelmesi engellenmiş olunur. Birinci rastgele sayı üretecinden çıkan tur sayı değerleri kadar ilk turda ve ondan sonraki turlarda oluşan yeni S-kutularında sürekli olarak yerine koyma metodu uygulandıktan sonra veri şifrelenmiş olur.

Tur sayılı S-kutusu ile şifreleme akış diyagramı Şekil 4.5'te gösterilmektedir. Şifreli veri, şifreleme algoritmasının tersine işlemler yapılarak deşifreleme işlemine tabi tutulur ve bu şekilde orijinal veri elde edilir.



Şekil 4.5. Tur sayılı S-Kutusu yönteminin akış diyagramı

4.4.1. Tur sayılı S-kutusu yöntemi ile metin şifreleme

Örnek olarak metnin ilk karakteri "t" olarak alınsın. "t" karakterinin ASCII tablosundaki desimal karşılığı 116, heksadesimal karşılığı "74" olarak hesaplanır. Kaotik sistemden üretilen ilk rastgele sayı dizisinde ilk 3 bit "010" olarak alınsın. Bu değerin desimal karşılığı 2 olduğu için 3 tur yerine koyma metodu uygulanır. Kaotik sistemden üretilen ikinci rastgele sayı dizisinden S-kutusu oluşturulur. Karakterin hesaplanan heksadesimal "74" değeri, ilk turda üretilen S-kutusunda 7. satır 4. sütuna denk gelen "DE" değeri olarak bulunur. Bundan sonraki turlarda S-kutusunun içeriğinin değerleri heksadesimal olarak "01" azaltılacak şekilde her turda yeni bir S-kutusu oluşturulur. İkinci turda D. satır E. sütun "B8" değerine karşılık gelir. Üçüncü turda ise B. satır 8.sütun "5C" değerine karşılık gelir ve bu değer gerekli desimal ve ASCII tablo dönüşümleri sonucunda "\" karakterine karşılık gelir. Böylelikle "t" karakteri, "\" karakterine dönüştürülerek şifrelenmiş olur.

4.4.2. Tur sayılı S-kutusu yöntemi ile görüntü şifreleme

Örnek olarak görüntünün ilk kanalının ilk piksel değeri 38 olarak alınsın, bu değerin heksadesimal karşılığı "1C" olarak hesaplanır. Kaotik sistemden üretilen ilk rastgele sayı dizisinde ilk 3 bit "001" olarak alınsın. Bu değerin desimal karşılığı 1 olduğu için 2 tur yerine koyma metodu uygulanır. Kaotik sistemden üretilen ikinci rastgele sayı dizisinden

S-kutusu oluşturulur. İlk pikselin hesaplanan heksadesimal "1C" değeri, ilk turda üretilen S-kutusunda 1. satır C. sütuna denk gelen E7" değeri olarak bulunur. Bundan sonraki turda S-kutusunun içeriğinin değerleri heksadesimal olarak "01" azaltılır ve bir sonraki turda yeni bir S-kutusu oluşturulur. İkinci turda E. satır 7. sütun "49" değerine karşılık gelir ve bu değer desimal olarak 73 değerine karşılık gelir. Böylelikle 38 piksel değeri 73 değerine dönüştürülerek şifrelenmiş olur.

4.4.3. Tur sayılı S-kutusu yöntemi ile ses şifreleme

Örnek olarak ses verisinin ilk kanalının ilk değeri 0.3124 olarak alınsın, bu değerin desimal karşılığı 167, heksadesimal karşılığı "A7" olarak hesaplanır. Kaotik sistemden üretilen ilk rastgele sayı dizisinde ilk 3 bit "000" olarak alınsın. Bu değerin desimal karşılığı 0 olduğu için 1 tur yerine koyma metodu uygulanır. Kaotik sistemden üretilen ikinci rastgele sayı dizisinden S-kutusu oluşturulur. Ses verisinin ilk verisinin hesaplanan heksadesimal "A7" değeri, ilk turda üretilen S-kutusunda A. satır 7. sütuna denk gelen "5D" değeri olarak bulunur. Heksadesimal "5D" değeri desimal olarak 93'e eşittir ve bu da ses verisi olarak -0.2734 değeri olarak hesaplanır. Böylelikle 0.3124 değeri -0.2734 değerine dönüştürülerek şifrelenmiş olur.

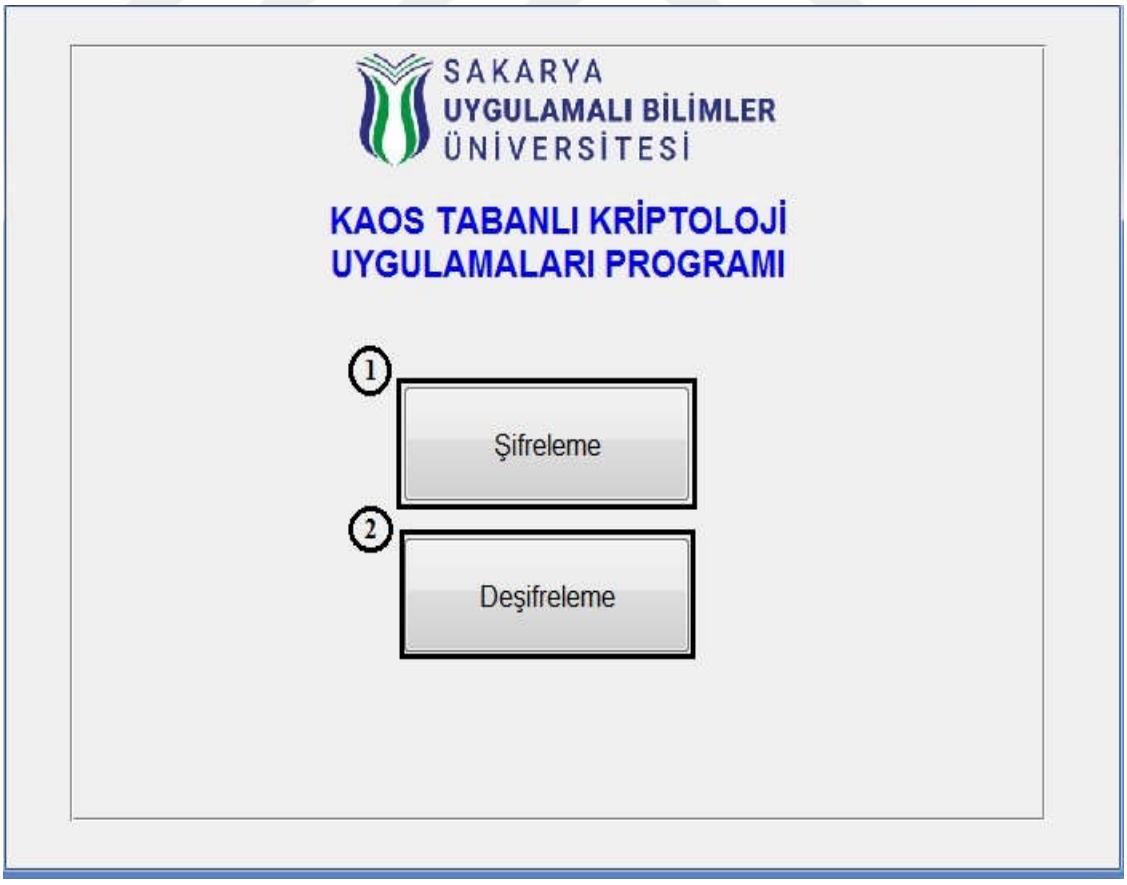
4.4.4. Tur sayılı S-kutusu yöntemi ile video şifreleme

Örnek olarak videonun şifrelenecek karesinin ilk kanalının ilk piksel değeri 145 olarak alınsın, bu değerin heksadesimal karşılığı "91" olarak hesaplanır. Kaotik sistemden üretilen ilk rastgele sayı dizisinde ilk 3 bit "011" olarak alınsın. Bu değerin desimal karşılığı 3 olduğu için 4 tur yerine koyma metodu uygulanır. Kaotik sistemden üretilen ikinci rastgele sayı dizisinden S-kutusu oluşturulur. İlk pikselin hesaplanan heksadesimal "91" değeri, ilk turda üretilen S-kutusunda 9. satır 1. sütuna denk gelen "9B" değeri olarak bulunur. Bundan sonraki turlarda S-kutusunun içeriğinin değerleri heksadesimal olarak "01" azaltılacak şekilde her turda yeni bir S-kutusu oluşturulur. İkinci turda 9. satır B. sütun "DC", üçüncü turda D. satır C. sütun "53" ve dördüncü turda 5. satır 3. sütunda "79" değeri elde edilir. Böylelikle bulunan heksadesimal "79" değeri, desimal 121 değeri olarak hesaplanır. Böylelikle 145 piksel değeri, 121'e dönüştürülerek ilk piksel değeri şifrelenmiş olur.

BÖLÜM 5. KAOS TABANLI YENİ BİR ÇOKLU ORTAM ŞİFRELEME YAZILIM ARACI TASARIMI

Tez çalışması için şifreleme ve deşifreleme yöntemlerinin kodlanması, kodlanan yöntemlerin kullanışlı bir şekilde uygulanabilmesi ve yapılan şifreleme analizlerinin daha uygun bir şekilde değerlendirilebilmesi için bir araya getirilmesi amaçları bir yazılım aracı tasarlanması ihtiyacını doğurmuştur. Bu yazılım aracı MATLAB® GUI programında tasarlanmıştır.

Şekil 5.1'de, MATLAB® GUI ortamında oluşturulan yazılım aracının açılış ekranının gösterimi mevcuttur.



Şekil 5.1. Yazılım aracının açılış ekranı

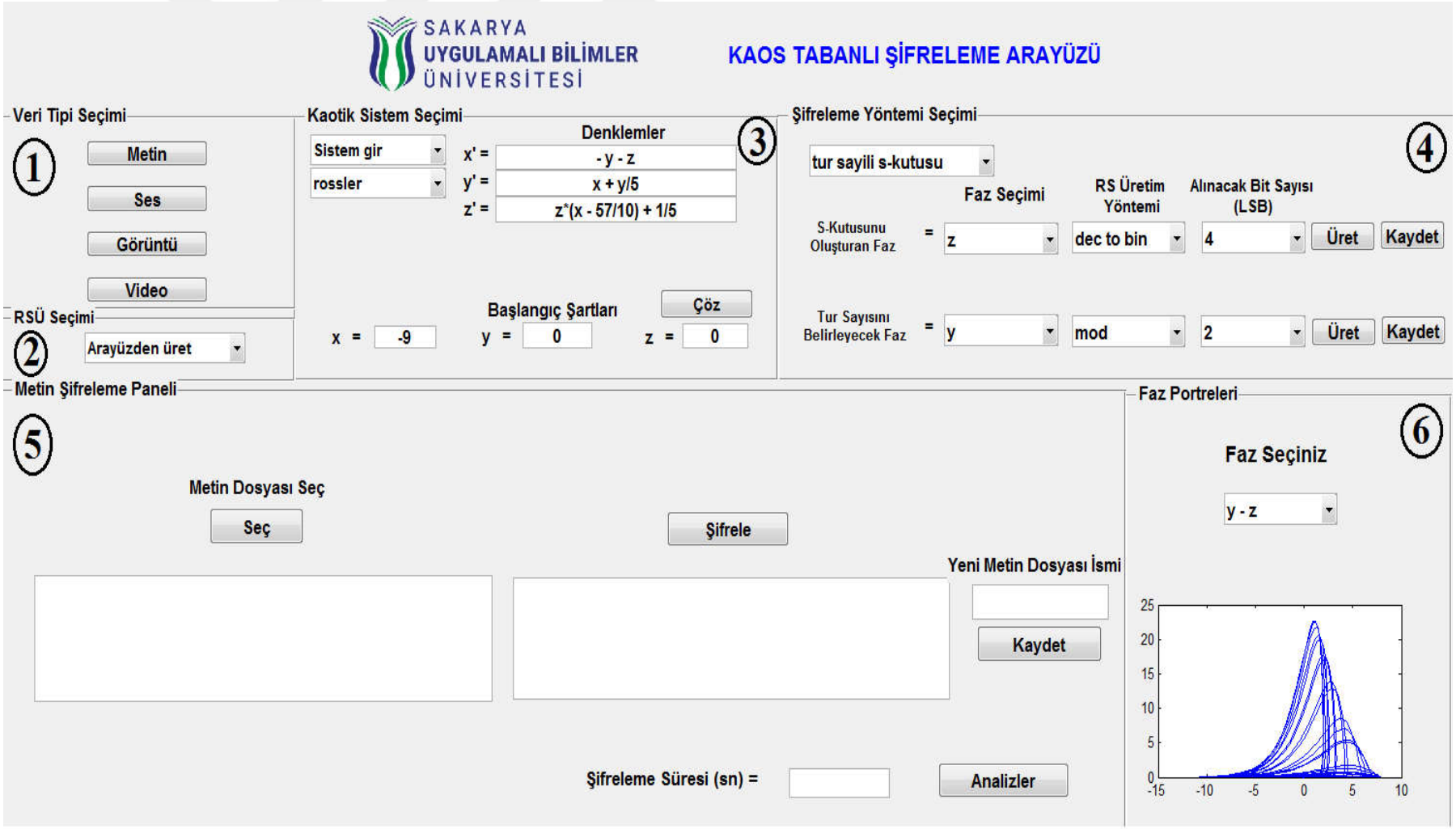
Yazılım aracının açılış ekranındaki seçimler sonucunda ayrıca iki adet alt panel sekmesi de oluşmaktadır. 1 numaralı buton ile şifreleme panel ekranı, 2 numaralı buton ile deşifreleme panel ekranı çağrılır.

5.1. Şifreleme ve Deşifreleme Panelleri

Şifreleme ve deşifreleme panelleri tasarım ve görsel olarak aynı şablon yapısındadır. 2 panel arasındaki temel fark ise şifreleme panelinde şifreleme algoritmaları, deşifreleme panelinde deşifreleme algoritmaları kullanılmasıdır ve bu ters işlemlerin yapıldığı aynı alandaki panel yazılarında bazı farklılıklar mevcuttur.

Tez çalışmasının bu bölümünde şifreleme ve deşifreleme panellerinin tanıtımında görsel ve metinsel tekrarlamaların oluşmaması için sadece şifreleme paneli baz alınarak bir tanıtım gerçekleştirilmiştir. Şifreleme panelleri tanıtımında kullanılan komut, buton, pencere ve yönergelerin anlatılan özellikleri aynı şekilde deşifreleme paneli için de geçerlidir ve tezin 6. bölümünde gerçekleştirilen uygulamalarda deşifreleme işlemlerinin bulunduğu bölümlerde de bu panel elemanları gösterilmiştir.

Şekil 5.2'de yazılım aracının şifreleme paneli görseli verilmiştir.



Şekil 5.2. Yazılım aracının şifreleme paneli

Şifreleme paneli Şekil 5.2'de gösterildiği gibi 6 kısımdan oluşmaktadır.

1 numara "Veri Tipi Seçimi" kısmıdır. Şifrelenecek dosya tipleri bu kısımda seçilir.

2 numara "RSÜ Seçimi" kısmıdır. Bu kısımda şifreleme işlemi yapmak için rastgele sayıların seçimi 2 şekilde gerçekleştirilir. İlk seçenek, rastgele sayıların yazılım aracından oluşturulmasıdır. İkinci seçenek ise rastgele sayıların "*txt*" dosya girişi ile girilmesidir.

3 numara "Kaotik Sistem Seçimi" kısmıdır. Bu kısımda şifrelemede kullanılacak olan kaotik sistemler ile ilgili seçenekler mevcuttur. "Sistem gir" seçeneği ile yazılım aracında bulunan mevcut sistemler kaydedilen başlangıç şartlarıyla ya da başlangıç şartları değiştirilerek kullanılabilir. "Elle gir" seçeneği ise kullanıcı tarafından şifrelemede kullanılmak üzere sistem derecesi 3, 4 veya 5 olacak şekilde yeni bir kaotik sistemin kaydedilmesine olanak sağlar.

4 numara Şekil 5.2'de "Şifreleme Yöntem Seçimi" kısmıdır. Bu kısımda, 2. kısımdaki seçimler sonucu farklı formlarda oluşan iki adet panel ekrana gelir. 2. kısımda "arayüzden üret" seçeneğinin seçilmesi sonucu Şekil 5.2'deki ekran oluşur. Oluşan 4. kısım ekranında hangi şifreleme yönteminin, hangi fazların, hangi rastgele sayı üretme metodunun kullanılacağı ve kaç bitlik hassasiyet ile rastgele sayı üretileceği belirlenir. Üretilen rastgele sayılar "kaydet" seçeneği ile "*txt*" dosya formatı olarak kaydedilebilir. 2. kısımda "Textten al" seçeneğinin seçilmesi sonucu Şekil 5.3'te verilen 4. kısım ekranı oluşur.

Şekil 5.3. Textten al seçiminin yapılmasıyla oluşan "Şifreleme Yöntem Seçimi" ekranı

Oluşan bu 4. kısım ekranında kullanılacak şifreleme yöntemi seçilir. "Rastgele Sayı Seç" dosya yolu bulma seçeneği ile kullanıcı rastgele sayıların girişini "*txt*" uzantılı bir dosyayı seçerek gerçekleştirebilir. Bu seçim sonucunda seçilen rastgele sayıların başlangıcındaki ile bitişindeki belirli sayıda değerler ve kaç adet sayının "*txt*" dosyasından çekildiği butonun yanındaki gösterge kutucuğunda gösterilir.

5 numara şifreleme panelinde "Şifreleme Panelleri Kısmı" olarak yer almaktadır. Bu kısımda çoklu ortam verilerinin şifreleme işlemleri gerçekleştirilir. Ayrıca her bir çoklu ortam verisi için analiz sonuçlarını gösteren panelleri çağıran butonlar da bu kısımda bulunmaktadır.

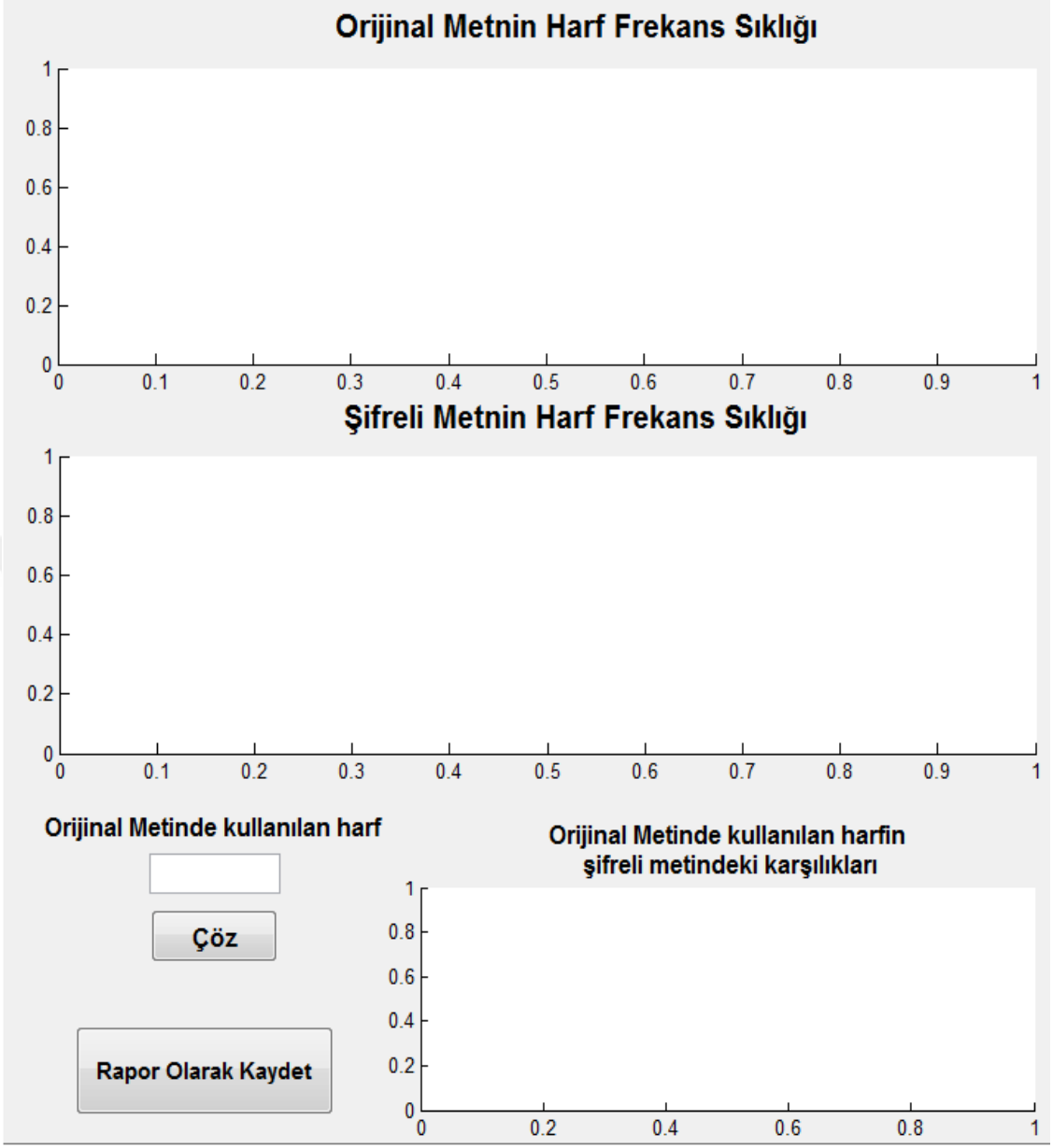
6 numaralı kısım "Faz Portreleri" kısmıdır. Bu kısım, yazılım aracının içerisinde bulunan veya kullanıcı tarafından sonradan eklenen kaotik sistemlerin 2 boyutlu faz portrelerini göstermektedir.

5.2. Analiz Panelleri

Analiz panelleri, şifreleme panelinde her bir çoklu ortam verisinin şifreleme kısmında bulunan analiz butonları ile çağırılan panel ekranlarıdır. Yazılım aracın içerisinde metin şifreleme analiz paneli, ses şifreleme analiz paneli ve görüntü & video şifreleme analiz paneli olarak 3 analiz paneli mevcuttur.

- **Metin şifreleme analiz paneli**

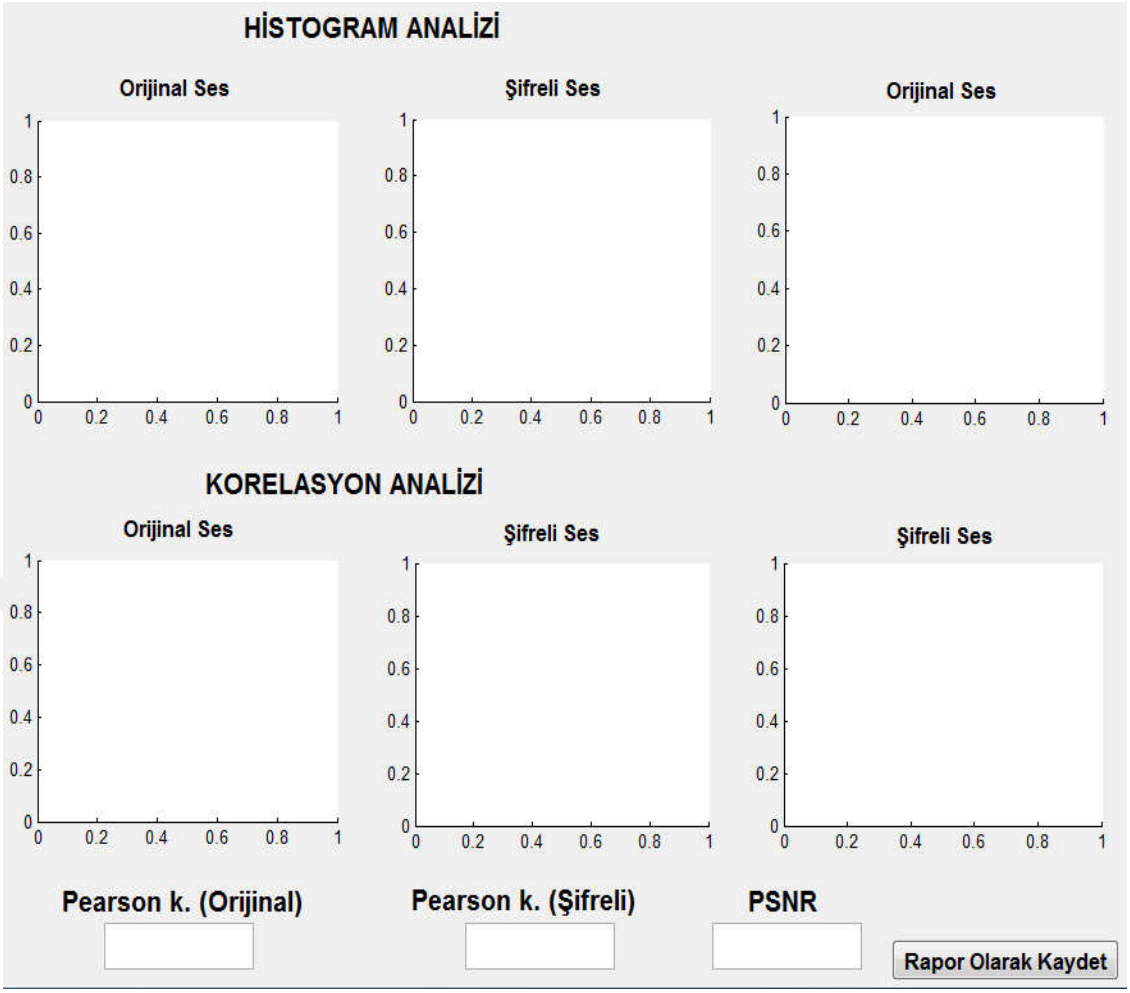
Metin şifreleme analiz panelinde hem orijinal metin verisinin hem de şifrelenmiş metin verisinin harf frekans sıklığı gösterilmektedir. Ayrıca orijinal metinde bulunan karakterlerin şifreli metinde hangi karakterlere dönüştüğünü gösteren bir grafik de mevcuttur. Yapılan metin şifreleme analizleri "Rapor olarak kaydet" butonuyla "docx" formatında kaydedilebilir. Yazılım aracının metin şifreleme analiz paneli Şekil 5.4'te verilmiştir.



Şekil 5.4. Yazılım aracının metin şifreleme analiz paneli

- **Ses şifreleme analiz paneli**

Ses şifreleme analiz panelinde hem orijinal ses verisinin hem de şifrelenmiş ses verisinin histogram analizi, korelasyon analizi, pearson korelasyon katsayısı ve PSNR analizi mevcuttur. Yapılan ses şifreleme analizleri "Rapor olarak kaydet" butonuyla "docx" formatında kaydedilebilir. Yazılım aracının ses şifreleme analiz paneli Şekil 5.5'te verilmiştir.

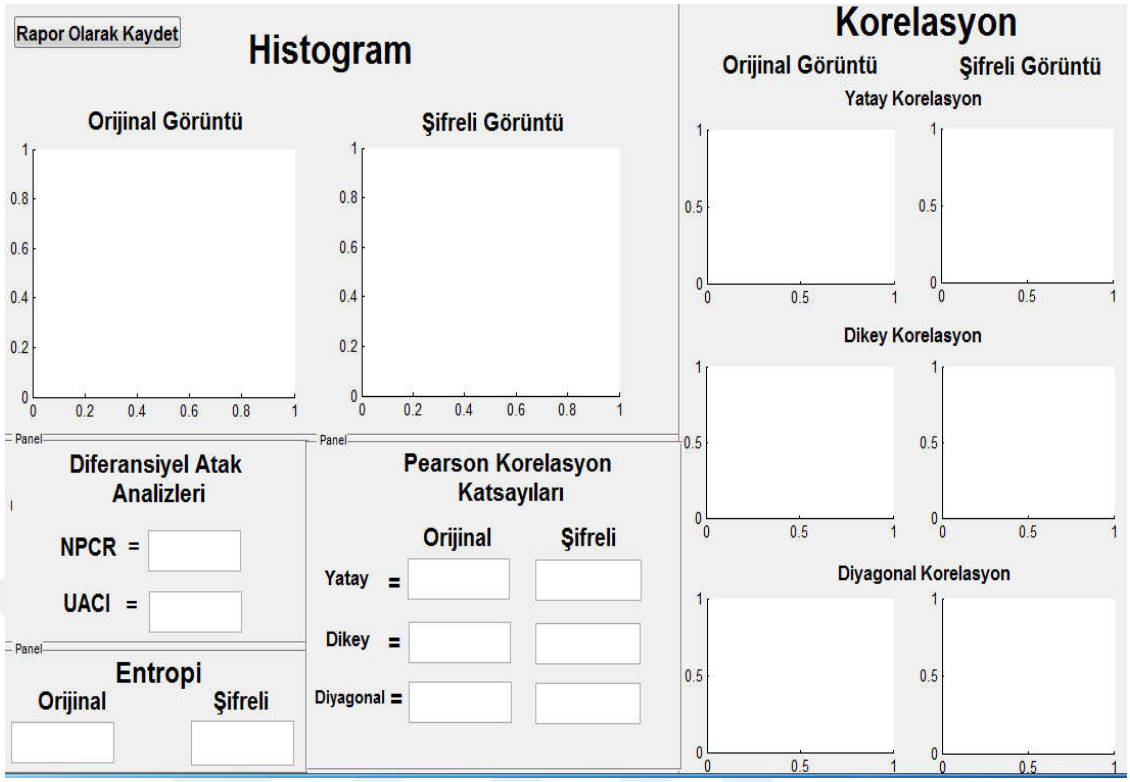


Şekil 5.5. Yazılım aracının ses şifreleme analiz paneli

- **Görüntü & video şifreleme analiz paneli**

Görüntü şifreleme analiz panelinde hem orijinal görüntü hem de şifrelenmiş görüntünün histogram analizi, korelasyon analizleri, diferansiyel atak analizleri değerleri, pearson korelasyon katsayı değerleri ve entropi değerleri mevcuttur.

Video dosyalarının şifrelenmesi sonucunda şifrelenmiş olan kare grubundan istenen görüntülerin analizleri de bu analiz panelinde gösterilir. Şifrelenen video kare grubundan bir görüntü ile o görüntünün orijinal halinin histogram analizi, korelasyon analizleri, diferansiyel atak analizleri değerleri, pearson korelasyon katsayı değerleri ve entropi değerleri bulunur. Yapılan görüntü ve video şifreleme analizleri "Rapor olarak kaydet" butonuyla "*docx*" formatında kaydedilebilir. Yazılım aracının görüntü ve video şifreleme analiz paneli Şekil 5.6'da verilmiştir.



Şekil 5.6. Yazılım aracının görüntü & video şifreleme analiz paneli

BÖLÜM 6. KAOS TABANLI ÇOKLU ORTAM ŞİFRELEME ARACIYLA YAPILAN UYGULAMALAR

Bu bölümde, tez çalışması kapsamında önerilen her bir şifreleme yöntemi ile farklı bir çoklu ortam verisinin (metin, görüntü, ses, video) şifreleme ve deşifreleme işlemlerinin yapıldığı 4 uygulama gerçekleştirilmiştir. Şifreleme ve deşifreleme uygulamalarının gerçekleştirildiği bilgisayarın özellikleri Tablo 6.1'de verilmiştir.

Tablo 6.1. Uygulamaların gerçekleştirildiği bilgisayarın özellikleri

İşlemci	Intel İ7-3630QM
İşlemci frekansı	2.40 GHz
Çekirdek sayısı	8
Bellek	16 GB
İşletim Sistemi	Windows 10 - 64 bit

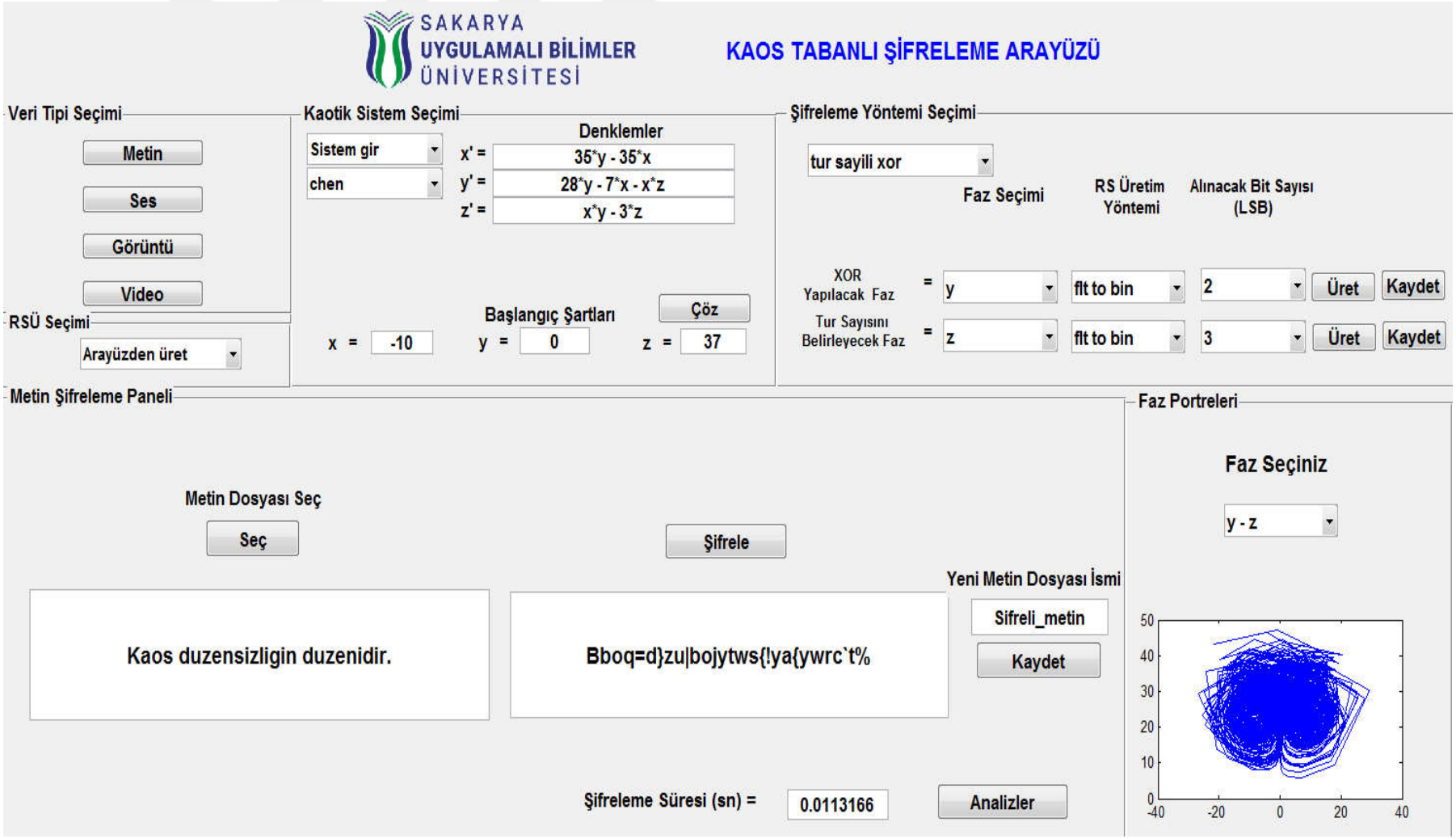
6.1. Tur Sayılı XOR Yöntemi ile Metin Şifreleme ve Deşifreleme Uygulaması

Bölüm 4.2.1'de anlatılan Tur sayılı XOR şifreleme yöntemi kullanılarak metin şifreleme uygulaması gerçekleştirilmiştir. Uygulamada kaotik sistem olarak Chen denklemi seçilmiştir. Sonrasında her veri için XOR işlemini yapacak faz ve XOR işlemi yapılması için gereken tur sayısını belirleyen faz seçimleri gerçekleştirilerek iki adet sayı dizisi elde edilmiştir. Sayı dizilerinin üretiminde her iki faz için de RSÜ yöntemi olarak kayan noktalı sayı yöntemi kullanılmıştır. Rastgele sayıların üretiminde hassasiyet bit değerleri 2 ve 3 olarak seçilmiştir. Tablo 6.2'de, kaotik sistemden elde edilen iki sayı dizisinin NIST 800-22 testi sonuçları gösterilmektedir. Test sonuçları neticesinde kaotik sistemden elde edilen sayı dizilerinin rastgele oldukları gözlemlenmiştir.

Tablo 6.2. Chen sisteminden üretilen değerlerin NIST 800-22 testi sonuçları

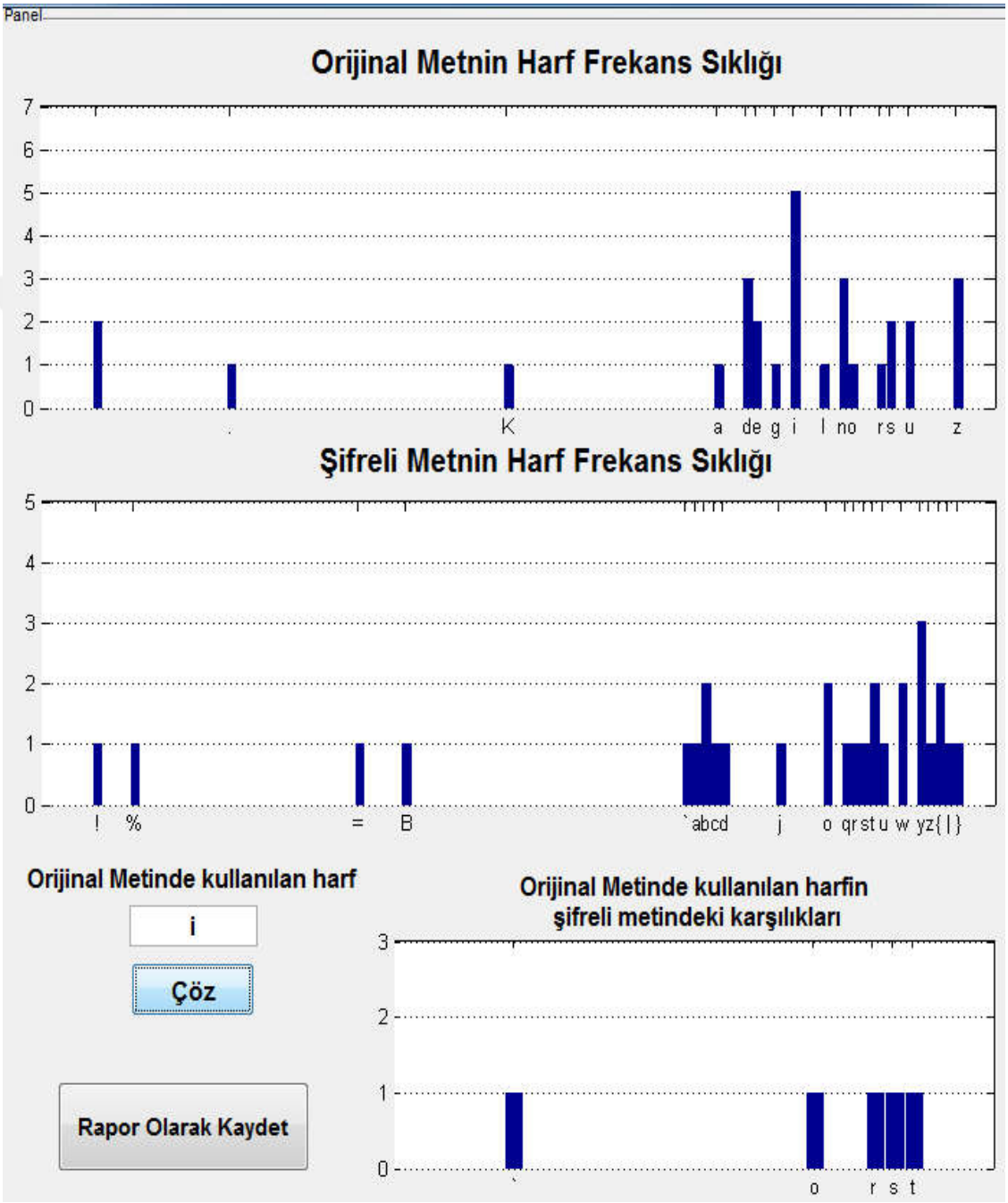
İstatistiksel Testler	**P-değeri (Y)**	**P-değeri (Z)**	**Sonuç**
Frekans testi	0.1700	0.5195	Başarılı
Blok frekans testi	0.3308	0.6508	Başarılı
Akış testi	0.4568	0.1060	Başarılı
Bir Blok içerisinde En Uzun Birler Akış Testi	0.6023	0.3492	Başarılı
İkili matris derece testi	0.4098	0.4227	Başarılı
Ayrık Fourier dönüşüm testi	0.2021	0.4088	Başarılı
Örtüşmeyen şablon eşleştirme testi	0.0723	0.1611	Başarılı
Örtüşen şablon eşleştirme testi	0.3820	0.8904	Başarılı
Maurer'in "evrensel istatistik" testi	0.6274	0.2211	Başarılı
Doğrusal karmaşıklık testi	0.2523	0.5502	Başarılı
Seri testi-1	0.7401	0.4157	Başarılı
Seri testi-2	0.9001	0.3719	Başarılı
Yaklaşık entropi testi	0.2314	0.2229	Başarılı
Birikimli toplamlar testi	0.2379	0.6680	Başarılı
Rastgele gezinimler testi	0.0648	0.0777	Başarılı
Rastgele gezinimler değişken testi	0.1540	0.4945	Başarılı

Elde edilen sayı dizilerinin rastgeleliği kanıtlandıktan sonra şifreleme işlemi gerçekleştirilmiştir. Şifrelenecek metin yazısı olarak "Kaos duzensizligin duzenidir." metni kullanılmıştır. Tur sayılı XOR yöntemi ile gerçekleştirilen uygulamanın metin şifreleme işlemi Şekil 6.1'de gösterilmiştir.



Şekil 6.1. Tur sayılı XOR yöntemi ile metin şifreleme işlemi

Şifreleme tamamlandıktan sonra "kaydet" butonu ile şifreli metin, kullanıcı tarafından dosya ismi girilerek "*docx*" formatlı dosya şeklinde kaydedilmektedir. "Analizler" butonu seçilerek orijinal metin ile şifreli metnin analizini yapan bir panel çalıştırılır. Bu analiz paneli Şekil 6.2'de verilmiştir.



Şekil 6.2. Tur sayılı XOR yöntemi ile metin şifreleme analiz sonuçları

Şekil 6.2’deki panelde öncelikle orijinal metnin frekans sıklığı sonrasında ise şifreli metnin frekans sıklığı gözükmektedir. Bu analizlere göre orijinal metinde kullanılan 15 farklı karakter, şifrelenmiş metin verisinde 22 farklı karakter olarak oluşmuştur. Böylelikle şifreli metin verisinde karakter çeşitliliği artmış ve orijinal metnin karakter dağılımına göre daha homojen bir karakter dağılımı gerçekleşmiştir. Orijinal metinde kullanılan harfin şifreli metindeki karşılıkları adlı analizde ise kullanıcıdan orijinal metinde olan bir karakter girilmesi istenmektedir. Karakter girildikten sonra "Çöz" butonu ile girilen orijinal metindeki karakterin şifreli metindeki dönüşümünün karşılıkları verilmektedir. Şekil 6.2’de gösterilen analiz sonucunda kullanıcı tarafından girilen "i" karakteri orijinal metinde 5 kez kullanılırken, orijinal metindeki her bir "i" karakteri şifreleme sonucunda " ` ", "o", "r", "s" ve "t" karakterlerine dönüşmüştür.

Orijinal metnin harf frekans sıklığı ile şifreli metnin harf frekans sıklığı analiz sonuçlarına bakarak başarılı bir metin şifreleme işlemi yapıldığı söylenebilir. Aynı zamanda analiz panelinde bulunan "Rapor Olarak Kaydet" butonu ile yapılan bu analizler Word dosyasına aktarılmaktadır.

Şekil 6.3’te metin deşifreleme algoritmasının uygulaması gösterilmektedir. Şifreleme işlemiyle şifrelenen metin, yeni bir kullanıcıya gönderildikten sonra kullanıcı deşifreleme panelinde doğru seçimleri (kaotik sistem, başlangıç şartları, rastgele sayı üreteci yöntemi, rastgele sayı üreteci yönteminde kullanılan faz, rastgele sayı üreteci yönteminde kullanılan hassasiyet bit değeri, şifreleme yöntemi) girdikten sonra şifrelenmiş metin deşifre edilerek orijinal metin elde edilir.

Şekil 6.3. Tur sayılı XOR yöntemi ile metin deşifreleme işlemi

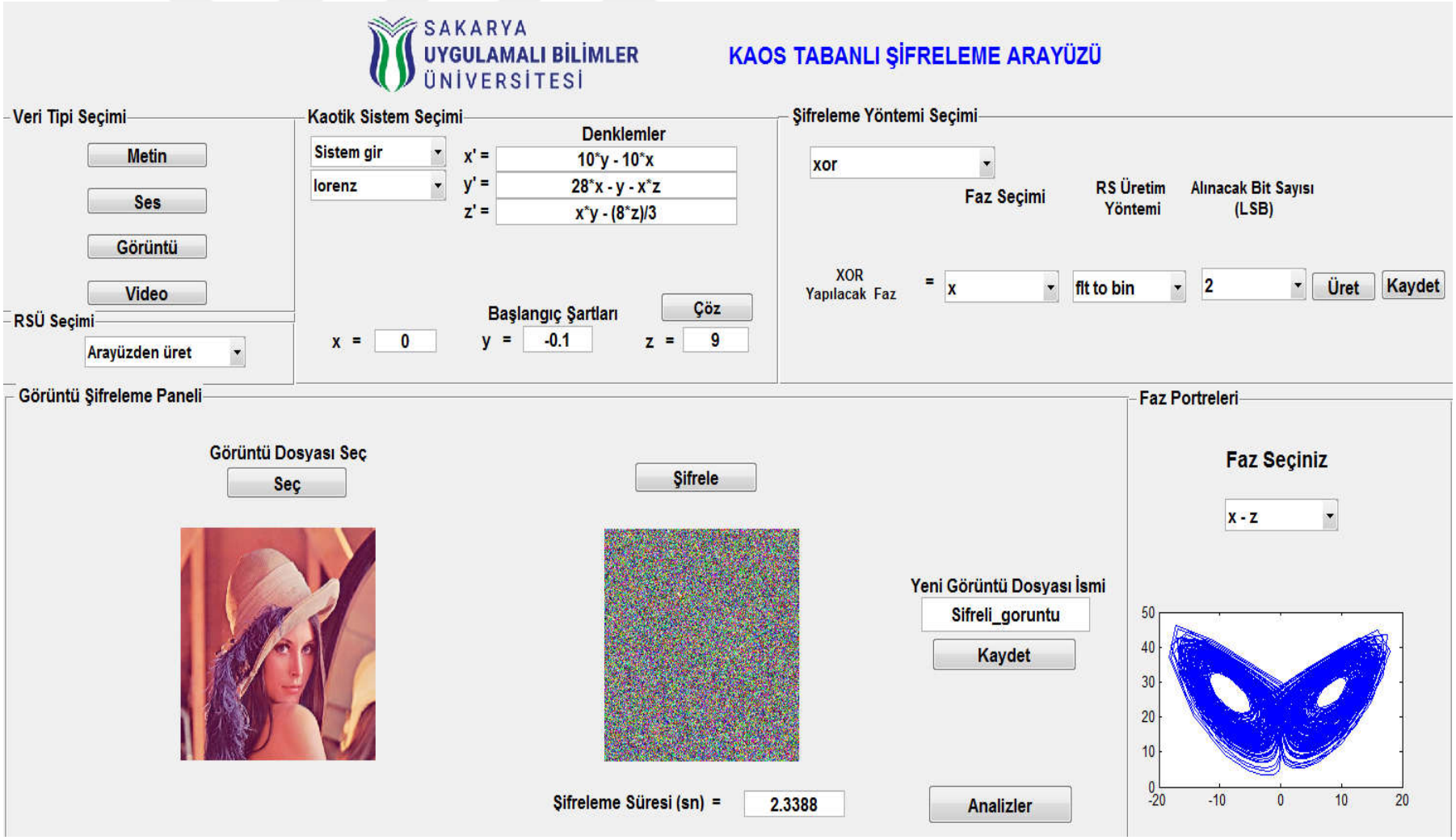
6.2. XOR Yöntemi ile Görüntü Şifreleme ve Deşifreleme Uygulaması

Bölüm 4.1.2'de anlatılan XOR şifreleme yöntemi kullanılarak kullanıcının seçtiği 512 x 512 boyutlarındaki görüntünün 3 kanallı şifreleme uygulaması gerçekleştirilmiştir. Uygulamada kaotik sistem olarak Lorenz denklemi seçilmiştir. XOR işlemini yapacak faz seçilerek rastgele sayı dizisi elde edilmiştir. Rastgele sayıların üretiminde hassasiyet bit değeri 2 olarak seçilmiştir. Sayı dizisinin üretiminde kullanılan faz için RSÜ yöntemi olarak kayan noktalı sayı yöntemi kullanılmıştır. Elde edilen sayı dizisinin NIST 800-22 testi sonuçları Tablo 6.3'te gösterilmektedir.

Tablo 6.3. Lorenz sisteminden üretilen değerlerin NIST 800-22 testi sonuçları

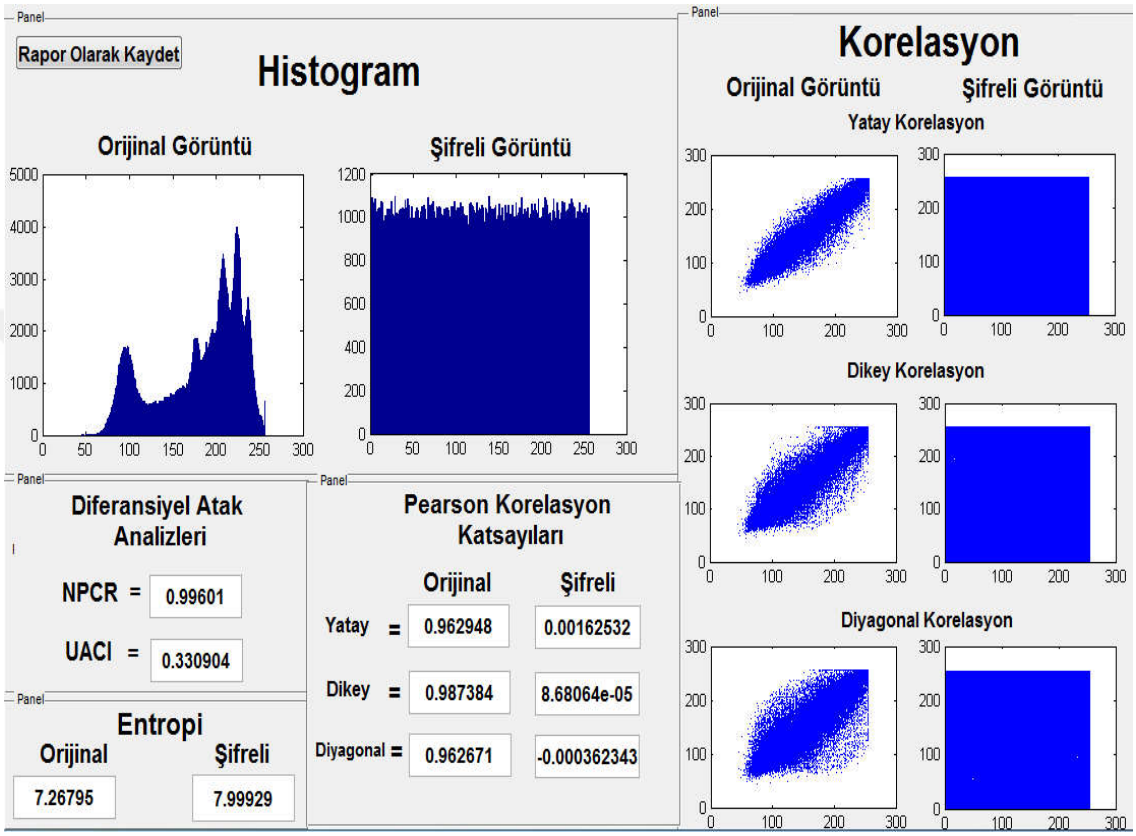
İstatistiksel Testler	**P-değeri (X)**	**Sonuç**
Frekans testi	0.8508	Başarılı
Blok frekans testi	0.2208	Başarılı
Akış testi	0.2055	Başarılı
Bir Blok içerisinde En Uzun Birler Akış Testi	0.3021	Başarılı
İkili matris derece testi	0.1297	Başarılı
Ayrık Fourier dönüşüm testi	0.5756	Başarılı
Örtüşmeyen şablon eşleştirme testi	0.3437	Başarılı
Örtüşen şablon eşleştirme testi	0.9398	Başarılı
Maurer'in "evrensel istatistik" testi	0.4062	Başarılı
Doğrusal karmaşıklık testi	0.7414	Başarılı
Seri testi-1	0.7877	Başarılı
Seri testi-2	0.9860	Başarılı
Yaklaşık entropi testi	0.7224	Başarılı
Birikimli toplamlar testi	0.9774	Başarılı
Rastgele gezinimler testi	0.1505	Başarılı
Rastgele gezinimler değişken testi	0.8554	Başarılı

Elde edilen sayı dizisinin rastgeleliği kanıtlandıktan sonra şifreleme işlemi gerçekleştirilmiştir XOR yöntemi ile gerçekleştirilen uygulamanın görüntü şifreleme işlemi Şekil 6.4'te gösterilmiştir.



Şekil 6.4. XOR yöntemi ile görüntü şifreleme işlemi

Şifreleme tamamlandıktan sonra kaydet butonu ile şifreli görüntü kullanıcı tarafından dosya ismi girilerek "*png*" formatlı dosya şeklinde kaydedilmektedir. "Analizler" butonu seçilerek, orijinal görüntü ile şifreli görüntünün güvenlik analizlerini yapan bir panel çalıştırılır. Bu analiz paneli Şekil 6.5'te verilmiştir.



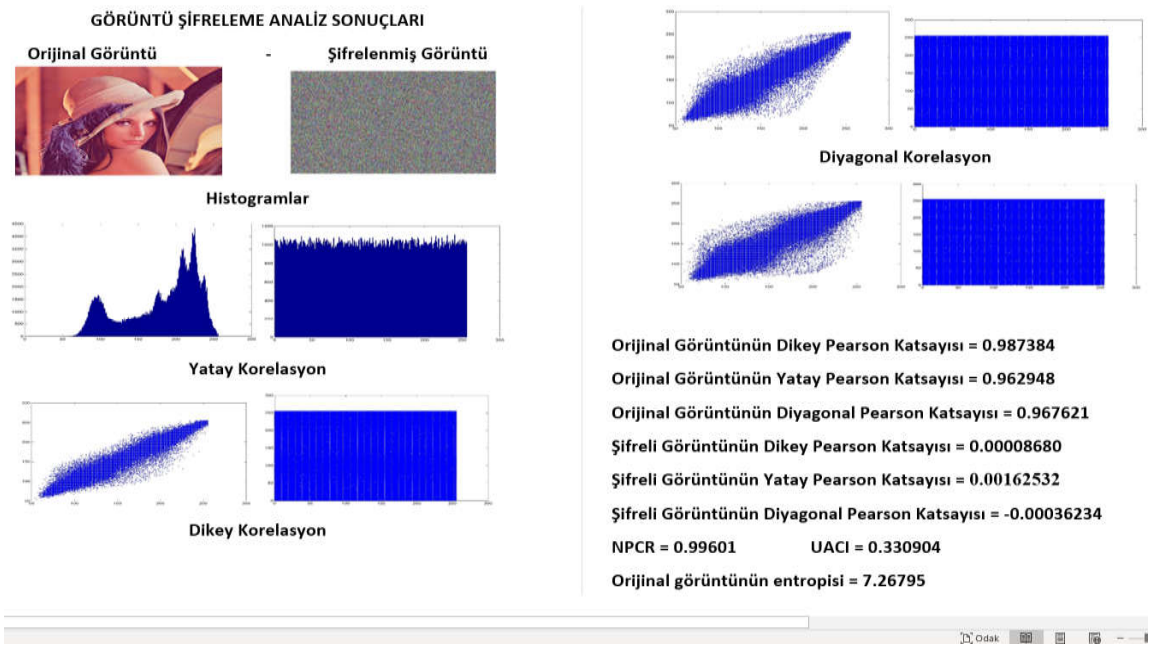
Şekil 6.5. XOR yöntemi ile görüntü şifreleme analiz sonuçları

Şekil 6.5'teki analiz panelinde orijinal görüntünün ve şifreli görüntünün "R" kanallarının analizleri gerçekleştirilmiştir. Öncelikle orijinal görüntünün ve şifreli görüntünün histogram eğrileri verilmiştir. Orijinal görüntünün histogramında bazı piksel değerleri daha ağırlıktayken şifreli görüntünün histogramında homojen bir değer dağılımı görülmektedir. Korelasyon analizlerinde ise yatay, dikey ve diyagonal korelasyon haritaları gösterilmektedir. Orijinal görüntünün 3 korelasyon haritasında da doğrusal bir grafik mevcuttur. Şifreli görüntünün 3 korelasyon haritasında ise 0 – 255 değer kümesinin tümüne yayılan homojen bir grafik mevcuttur. Böylelikle 3 doğrultuda gerçekleştirilen orijinal ve şifreli korelasyon haritalarıyla komşu veri değerleri arasındaki güçlü bağların zayıflatıldığı ispatlanmıştır. Yine 3 doğrultuda hesaplanan pearson korelasyon katsayı değerlerinin orijinal görüntü için 1'e çok yakın çıkması, şifreli görüntü için 0'a çok yakın

sonuçlar vermesi korelasyon haritalarının sonuçlarını desteklemektedir. NPCR ve UACI değerleri 0.99601 ile 0.330904 olarak elde edilmiştir. Bu değerlerle orijinal görüntü ile şifreli görüntü arasında değiştirilen piksellerin sayısı ve değiştirilen piksellerin ortalama değeri hakkında eşik değer olarak belirlenen değerlerin üstünde olan sonuçlara ulaşılmıştır. Analizi yapılan şifreli görüntü için en yüksek entropi değeri 8'dir. Bu değerde belirsizlik yani bilgiyi erişememe durumu en üst seviyededir. Analiz sonucunda entropi değeri 7.99929 olarak bulunmuş ve bu değer ile çıkabilecek en yüksek entropi değerine çok yaklaşılmıştır.

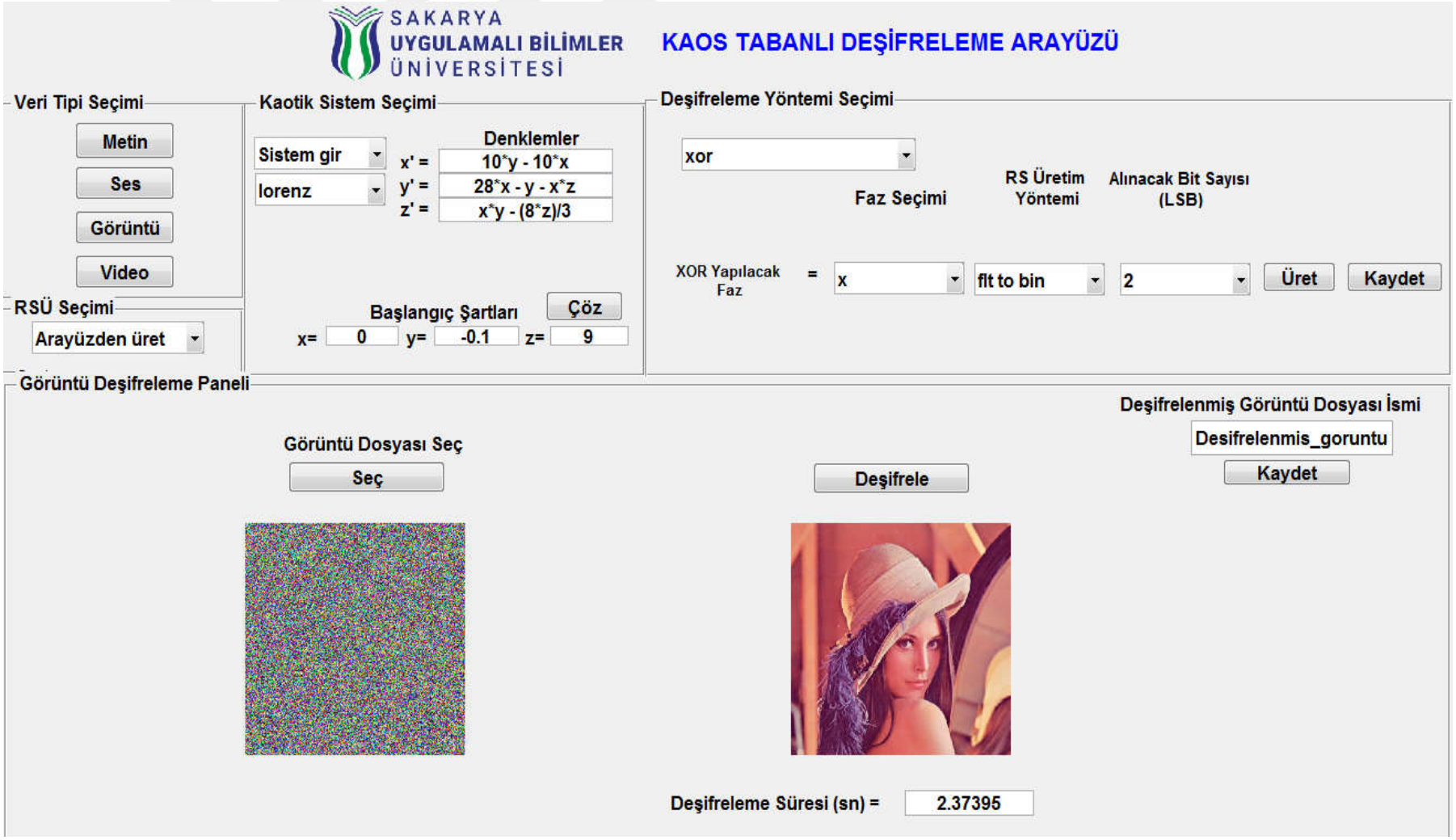
Analiz sonuç değerlerine bakarak başarılı bir görüntü şifreleme işlemi yapıldığı söylenebilir.

Panelde bulunan "Rapor Olarak Kaydet" butonu ile bu analizlerin Word dosyasına aktarımı gerçekleştirilir. Şekil 6.6'da analizin rapor çıktısı verilmiştir.



Şekil 6.6. XOR yöntemi ile görüntü şifreleme analizlerinin rapor çıktısı

Şekil 6.7'de görüntü deşifreleme uygulaması gösterilmektedir. Şifreleme işlemiyle şifrelenen görüntü, yeni bir kullanıcıya gönderildikten sonra kullanıcı deşifreleme panelinde doğru seçimleri (kaotik sistem, başlangıç şartları, rastgele sayı üretimi seçenekleri, şifreleme yöntemi) girdikten sonra şifrelenmiş görüntü deşifre edilerek orijinal görüntü elde edilir.



Şekil 6.7. XOR yöntemi ile görüntü deşifreleme işlemi

Bu tez çalışmasında önerilen XOR, Tur sayılı XOR, S-kutusu & XOR ve Tur sayılı S-kutusu şifreleme algoritmalarıyla gerçekleştirilen görüntü şifreleme analiz sonuçları ile farklı kaynaklardan alınan aynı görüntü dosyası kullanılarak gerçekleştirilen şifreleme uygulamalarının analiz sonuçları bir karşılaştırma yapılabilmesi için Tablo 6.4'te verilmiştir. Karşılaştırma sonucunda tez çalışması kapsamında önerilen algoritmaların analizlerinin genel olarak başarılı sonuçlar verdiği gözlemlenmiştir.

Tablo 6.4. Görüntü şifreleme uygulamalarının analiz sonuçlarının karşılaştırılmaları

Metot	**Yatay korelasyon**	**Dikey korelasyon**	**Diyagonal korelasyon**	**UACI**	**NPCR**	**Entropi**
XOR	0.00162532	0.0000868	-0.0003623	0.330904	0.99601	7.99929
Tur sayılı XOR	0.00092587	0.0042361	0.00025758	0.330149	0.99602	7.99933
S-kutusu & XOR	0.00015864	0.0019884	-0.0012613	0.331047	0.99609	7.99914
Tur sayılı S-kutusu	-0.0006739	-0.000353	-0.0004896	0.330768	0.99611	7.99909
Liu ve ark. [26]	-0.0042	-0.036	0.0072	0.335603	0.99958	7.9901
Zhu ve ark. [72]	0.00089814	0.0012219	0.00367275	0.334815	0.99627	7.99934
Wang ve ark. [73]	0.000707	0.002165	0.014886	0.33456	0.99606	7.9994
Sayedzadeh ve ark. [74]	0.000550	0.000839	0.001124	0.334647	0.99683	7.99927
Wei ve ark. [75]	0.0054	0.0062	0.0017	0.334834	0.99586	7.9971
Hussain ve ark. [76]	−0.00675	−0.013694	−0.056334	0.334647	0.94683	-
Huang ve ark. [77]	−0.0050	−0.0006	−0.0025	0.2827	0.9954	7.9967
Sunil ve ark. [78]	-0.0058	0.0017	0.0035	0.278096	0.99572	7.9774

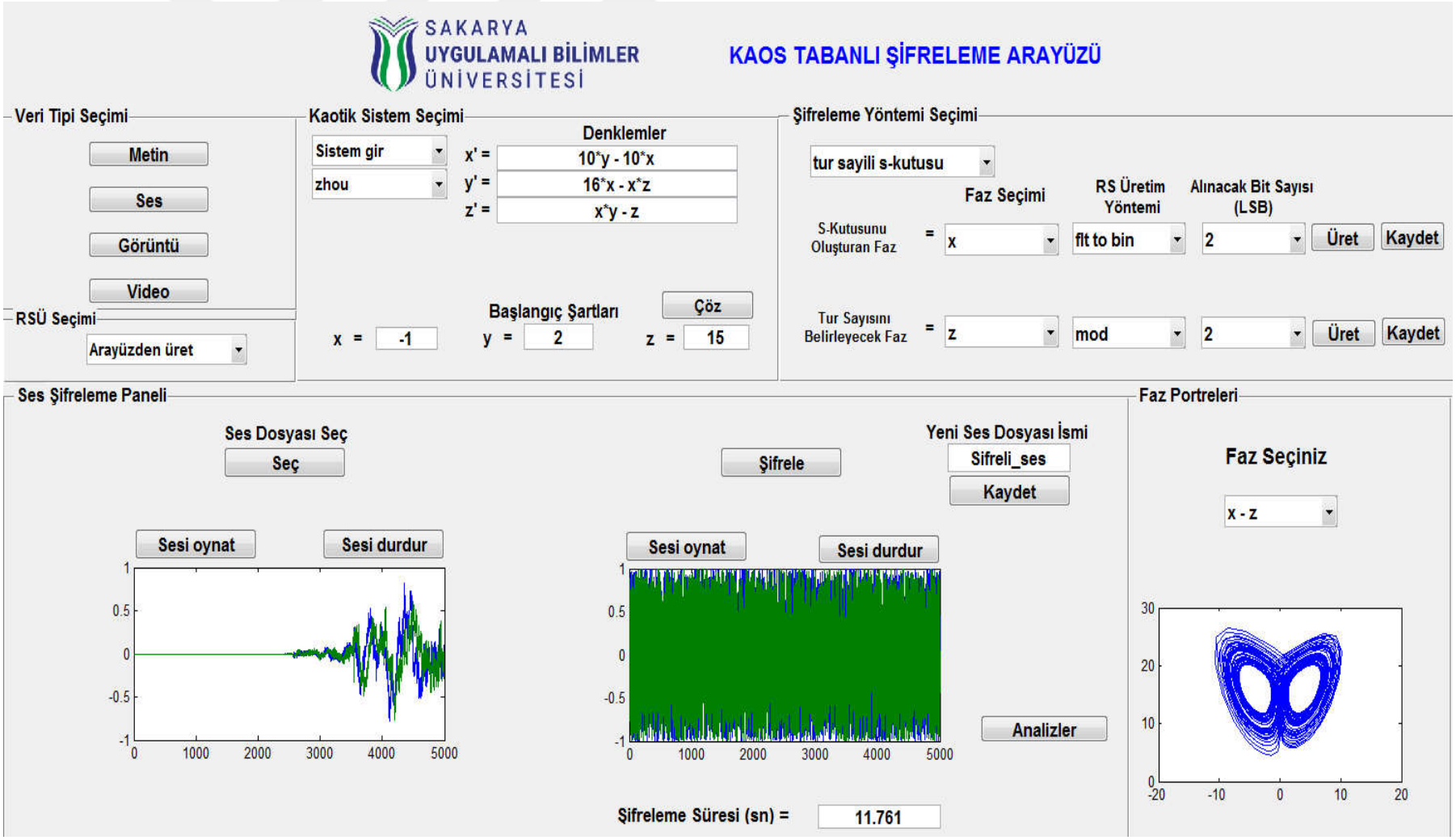
6.3. Tur Sayılı S-kutusu Yöntemi ile Ses Şifreleme ve Deşifreleme Uygulaması

Bölüm 4.4.3'te anlatılan tur sayılı S-kutusu şifreleme yöntemi kullanılarak kullanıcının seçtiği ses doyasının 2 kanallı şifreleme uygulaması gerçekleştirilmiştir. Uygulamada kaotik sistem olarak Zhou denklemi seçilmiştir. Sonrasında S-kutusunu oluşturan faz ve tur sayısını belirleyecek faz seçimleri yapılarak iki adet sayı dizisi elde edilmiştir. Sayı dizilerinin üretiminde S-kutusunu oluşturan faz için kayan noktalı sayı yöntemi, tur sayısını belirleyen faz için ise mod alma yöntemi kullanılmıştır. Rastgele sayıların üretiminde hassasiyet bit değerlerinin her ikisi de 2 olarak seçilmiştir. Şifrelenen 2 kanallı ses dosyasının örnekleme frekansı 44100'dür ve şifreleme işlemi ses dosyasının 2 saniyesini kapsayacak şekilde ayarlanmıştır.

Tablo 6.5. Zhou sisteminden üretilen değerlerin NIST 800-22 testi sonuçları

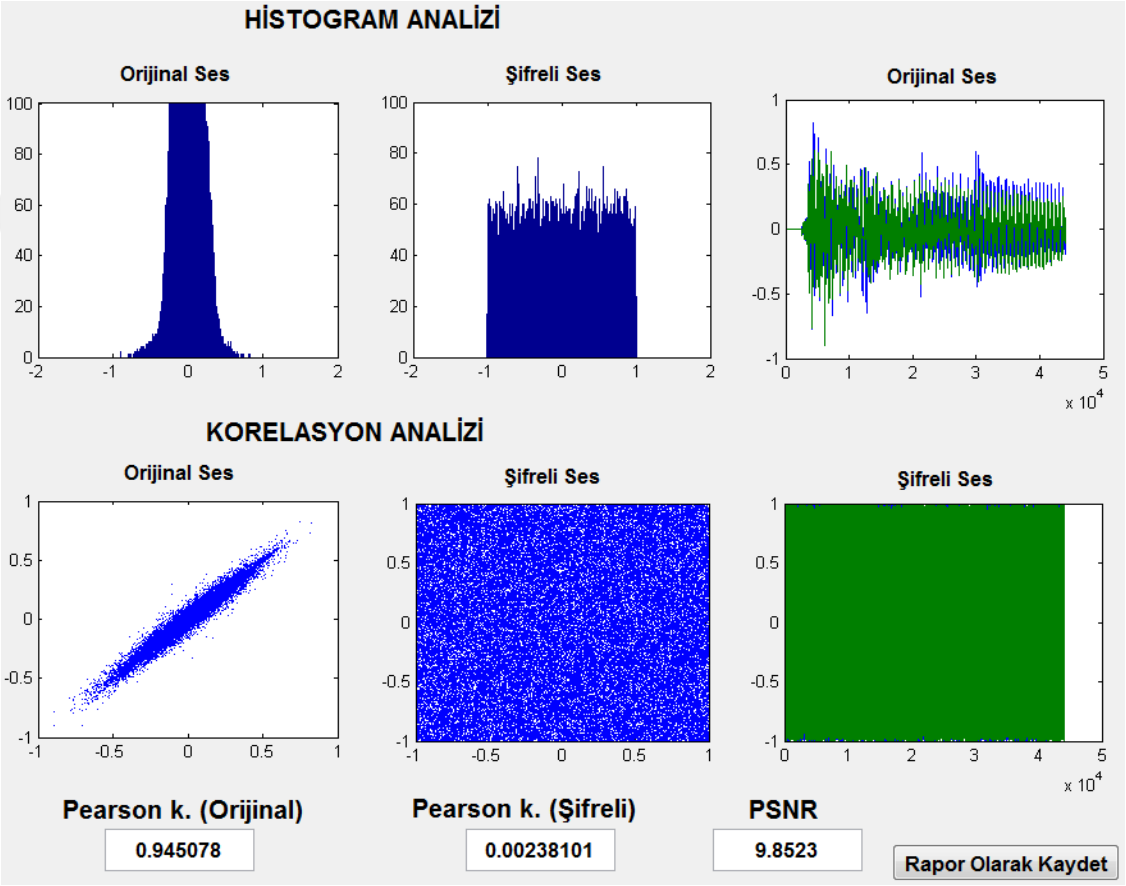
İstatistiksel Testler	**P-değeri (X)**	**P-değeri (Z)**	**Sonuç**
Frekans testi	0.8367	0.7444	Başarılı
Blok frekans testi	0.5046	0.5760	Başarılı
Akış testi	0.8196	0.3908	Başarılı
Bir Blok içerisinde En Uzun Birler Akış Testi	0.0850	0.1735	Başarılı
İkili matris derece testi	0.6676	0.4647	Başarılı
Ayrık Fourier dönüşüm testi	0.1863	0.0149	Başarılı
Örtüşmeyen şablon eşleştirme testi	0.0934	0.1293	Başarılı
Örtüşen şablon eşleştirme testi	0.4266	0.4244	Başarılı
Maurer'in "evrensel istatistik" testi	0.1864	0.0101	Başarılı
Doğrusal karmaşıklık testi	0.8689	0.7540	Başarılı
Seri testi-1	0.2622	0.9500	Başarılı
Seri testi-2	0.0939	0.9744	Başarılı
Yaklaşık entropi testi	0.1871	0.6403	Başarılı
Birikimli toplamlar testi	0.6801	0.9922	Başarılı
Rastgele gezinimler testi	0.4111	0.0646	Başarılı
Rastgele gezinimler değişken testi	0.5214	0.1540	Başarılı

Elde edilen sayı dizilerinin NIST 800-22 testi sonuçları Tablo 6.5'te gösterilmektedir. Elde edilen sayı dizilerinin rastgeleliği kanıtlandıktan sonra şifreleme işlemi gerçekleştirilmiştir. Tur sayılı S-kutusu yöntemi ile gerçekleştirilen uygulamanın ses şifreleme işlemi Şekil 6.8'de gösterilmiştir.



Şekil 6.8. Tur sayılı S-kutusu yöntemi ile ses şifreleme işlemi

Şifreleme tamamlandıktan sonra "Kaydet" butonu ile şifreli ses, dosya ismi kullanıcı tarafından girilerek "*wav*" uzantılı dosya şeklinde kaydedilmektedir. "Analizler" butonu, orijinal ses ile şifreli ses verilerinin analizini yapan bir panel çalıştırmaktadır. Bu analiz paneli Şekil 6.9'da verilmiştir. Orijinal ses dosyası ile şifrelenmiş ses dosyası, yazılım aracı üzerinde bulunan "Sesi oynat" butonuyla dinlenebilir, bu şekilde de şifreli ses ile orijinal ses arasındaki değişim net olarak fark edilebilir.



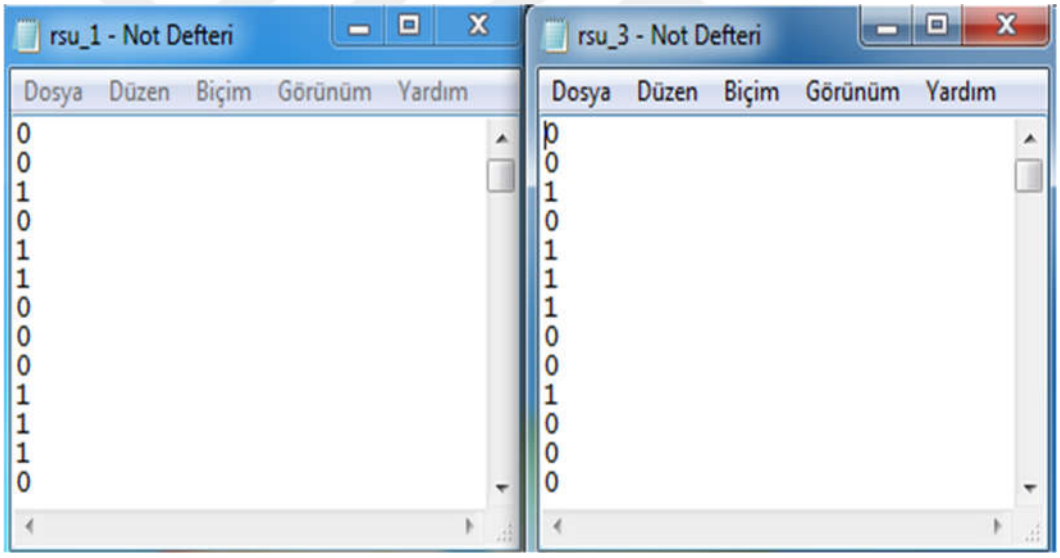
Şekil 6.9. Tur sayılı S-kutusu yöntemi ile ses şifreleme analiz sonuçları

Şekil 6.9'daki panelde öncelikle orijinal ses verisinin ve şifreli ses verisinin histogram eğrileri verilmektedir. Orijinal ses verisinin histogram grafiğinde -0.3 ile +0.3 arasında bulunan değerler ağırlıktayken şifreli ses histogram grafiğinde -1 ile +1 değerleri arasında homojen bir değer dağılımı sergilenmiştir. Korelasyon analizinde ise yatay korelasyon haritası gösterilmektedir. Korelasyon analizinde orijinal ses verisinin korelasyon haritasında daha doğrusal bir grafik mevcutken, şifreli ses verisinin korelasyon haritasında ise -1 ile +1 arasındaki değer kümesinin tümüne yayılan homojen bir grafik mevcuttur. Böylelikle yatay doğrultuda gerçekleştirilen orijinal ve şifreli korelasyon

haritalarıyla komşu veri değerleri arasındaki güçlü bağların zayıflatıldığı ispatlanmıştır. Yine yatay doğrultuda hesaplanan pearson korelasyon katsayı değerlerine bakıldığında, katsayı değerinin orijinal görüntü için 1'e çok yakın çıkması, şifreli görüntü için 0'a çok yakın sonuçlar vermesi korelasyon harita sonuçlarını destekler niteliktedir. PSNR değeri gürültü seviyesi olarak en iyi sonuç değeri olan 0'a yakın bir değer olarak hesaplanmıştır.

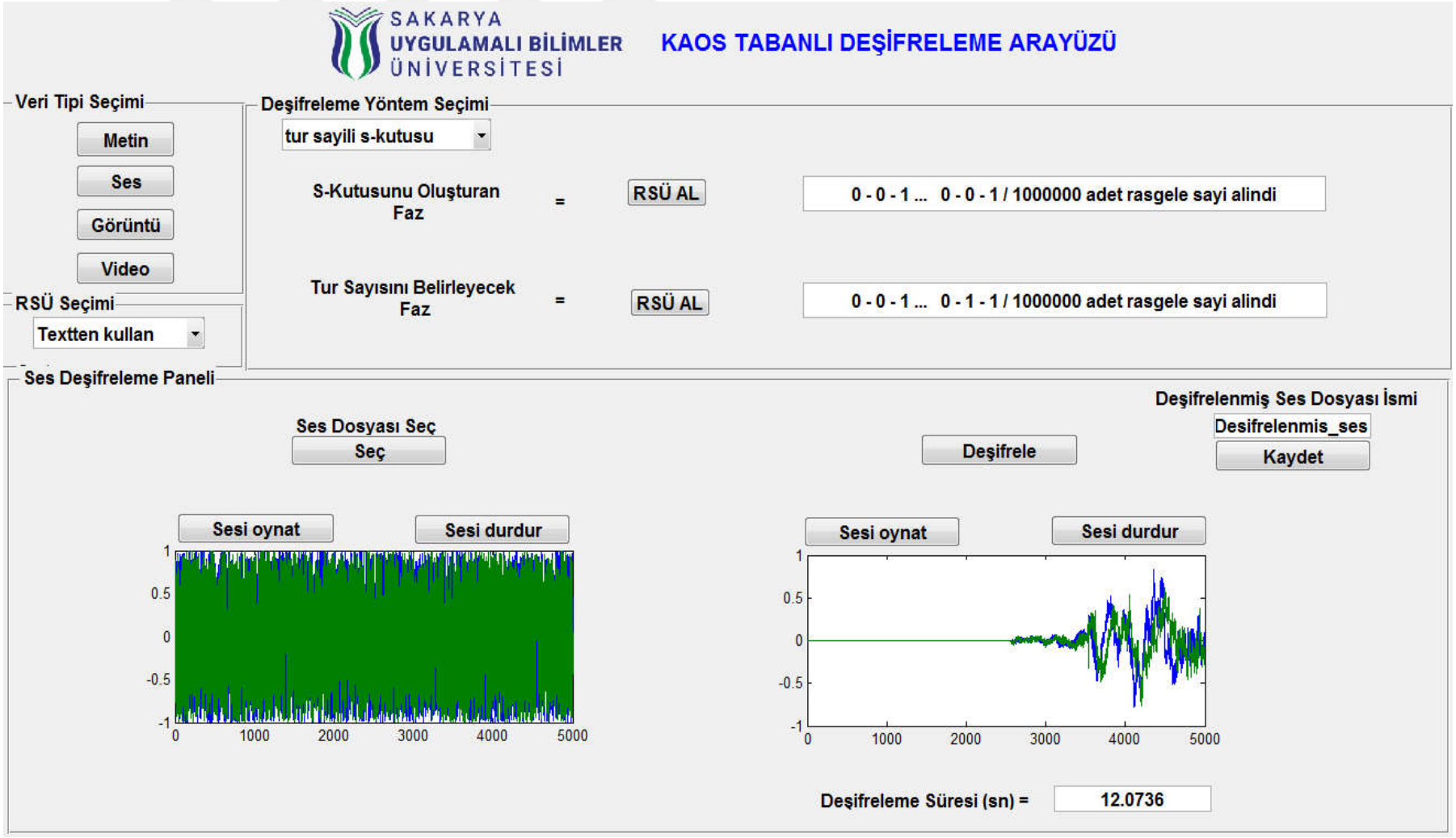
Yapılan analizlerin sonucunda ses verisinin başarılı bir şifreleme işleminden geçtiği söylenebilir Ayrıca panelde bulunan "Rapor Olarak Kaydet" butonu ile bu analizlerin Word dosyasına aktarımı gerçekleşmektedir.

Aynı zamanda şifreleme panelinde üretilen rastgele sayılar "Kaydet" butonu ile "*txt*" dosyasına aktarılabilir. Kaydedilen "*txt*" dosyaları Şekil 6.10'da gösterilmiştir. Bu şekilde kaydedilen rastgele sayılar yazılım aracında ilgili seçenekler seçilerek ses verisinin deşifre edilmesinde kullanılabilirler.



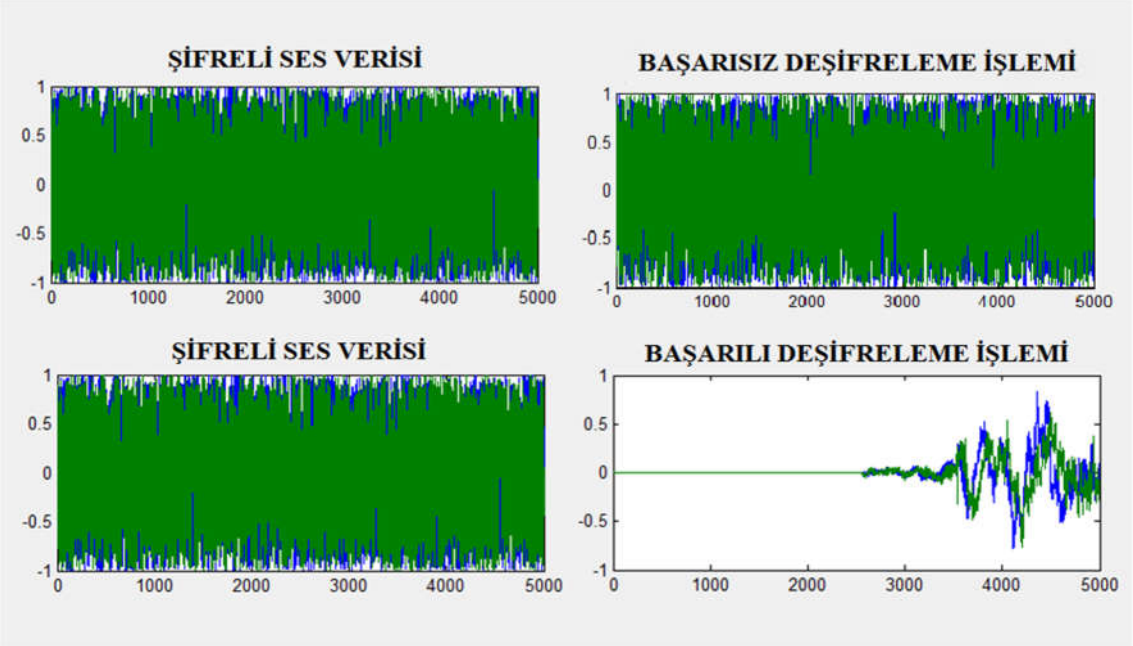
Şekil 6.10. Uygulamada kullanılan kaotik sistemin x ve z fazından elde edilen rastgele sayılar

Şekil 6.11'de ses verisi deşifreleme uygulaması gösterilmektedir. Şifreleme işlemiyle şifrelenen ses verisi ve "*txt*" dosyası içinde bulunan rastgele sayılar şifreyi çözen kullanıcıda mevcut ise kullanıcı deşifreleme panelinde geriye kalan doğru şifreleme yöntem seçimini de girerek şifrelenmiş ses verisi deşifre edilir ve böylelikle orijinal ses elde edilmiş olunur.



Şekil 6.11. Tur sayılı S-kutusu yöntemi ile ses deşifreleme işlemi

Kaosun tez çalışması için önerilen şifreleme uygulamalarının genelinde etkisini gösteren başlangıç şartlarına hassas duyarlılığı, ses verisinin şifrelendiği uygulama için bir örnek verilerek gösterilmiştir. Zhou kaotik sisteminin Şekil 6.8'deki başlangıç şartlarıyla elde edilen şifreli ses verisi için başka bir deşifreleme işlemi gerçekleştirilirken y fazının başlangıç değeri 0 yerine 10^{-14} olarak alınmıştır. Bu değer seçiminin dışında yazılım aracında deşifreleme için gerekli olan bütün doğru seçimler ((kaotik sistem, rastgele sayı üreteci yöntemi, rastgele sayı üreteci yönteminde kullanılan faz, rastgele sayı üreteci yönteminde kullanılan hassasiyet bit değeri, şifreleme yöntemi) girildikten sonra oluşan başarısız deşifreleme işleminin sonucu Şekil 6.12'de gösterilmiştir. Bu denli küçük bir değer değişiminin sonucunda deşifreleme işleminde bir başarı yakalanamamıştır. Şekilde y fazının başlangıç değeri 0 olarak girilmesiyle çıkan ses verisi de gösterilmektedir.



Şekil 6.12. Kaotik sistemlerde başlangıç şartlarının etkisini gösteren başarısız bir deşifreleme işlemi

6.4. S-kutusu & XOR Yöntemi ile Video Şifreleme ve Deşifreleme Uygulaması

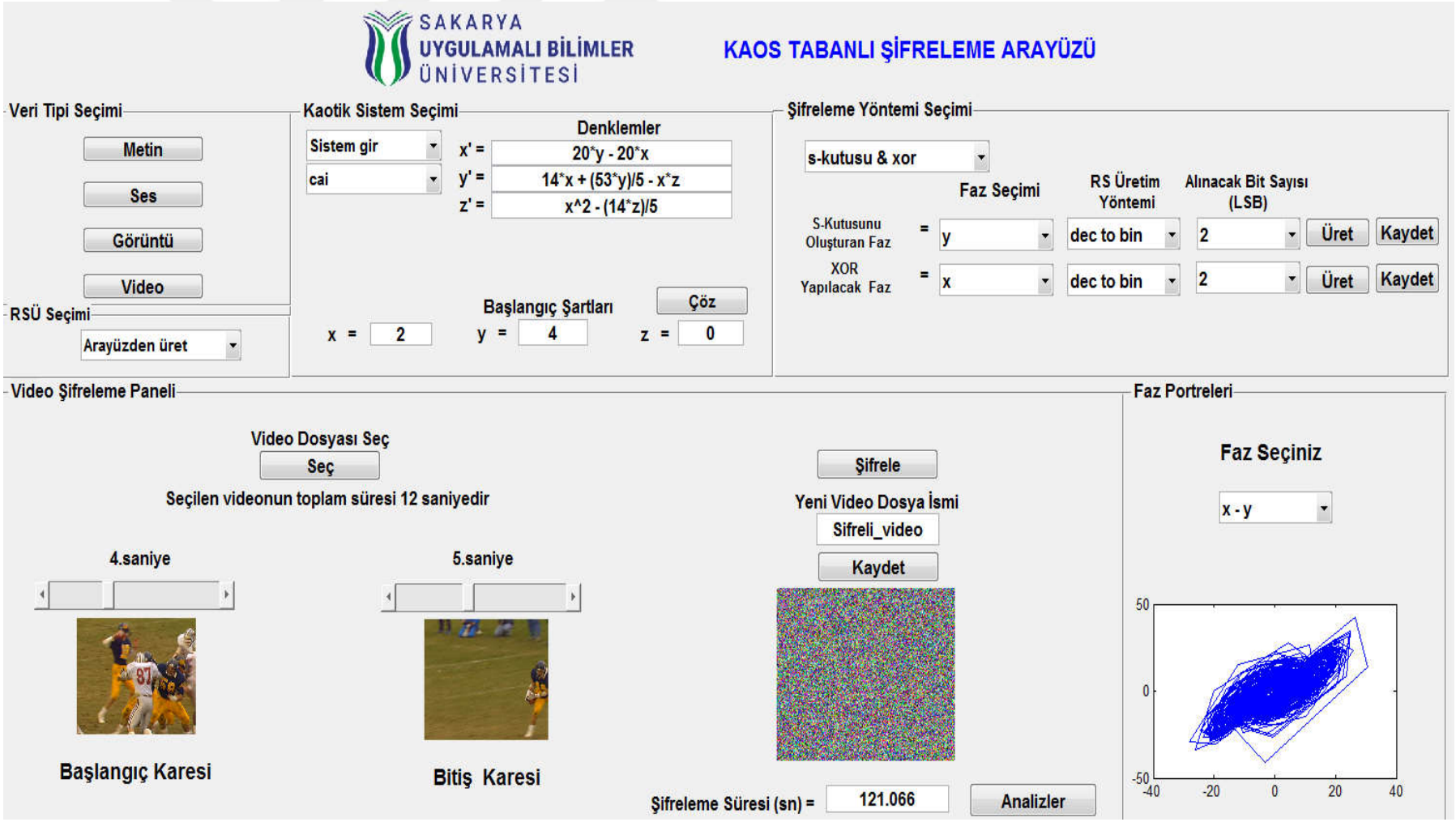
Bölüm 4.3.4'te anlatılan S-kutusu & XOR şifreleme yöntemi kullanılarak kullanıcının seçtiği video dosyasının 3 kanallı görüntü içeriklerinin şifreleme uygulaması gerçekleştirilmiştir. Uygulamada kaotik sistem olarak Cai denklemi seçilmiştir. Sonrasında S-kutusunu oluşturacak faz ile XOR işlemini yapacak faz seçimleri yapılarak iki adet sayı dizisi elde edilmiştir. Sayı dizilerinin üretiminde her iki faz için de RSÜ

yöntemi olarak desimalden ikilik tabana dönüştürme yöntemi kullanılmıştır. Rastgele sayıların üretiminde hassasiyet bit değerlerinin her ikisi de 2 olarak seçilmiştir. Video şifreleme uygulamasında şifrelenecek video seçildiğinde panele, video ile ilgili zaman bilgisi ve bu zaman sınırları dahilinde şifrelemenin hangi süreler arasında olacağını belirleyen kontrol elemanları gelmektedir. Şifrelenen video dosyası 352 x 288 boyutlarında, 30 fps özelliğine sahiptir. Şifreleme işlemi video dosyasının 2 saniyesini kapsayacak şekilde ayarlanmıştır. Bunun sonucunda şifreleme algoritması 60 tane 3 kanallı görüntü şifreleme işlemi gerçekleştirecektir.

Tablo 6.6. Cai sisteminden üretilen değerlerin NIST 800-22 testi sonuçları

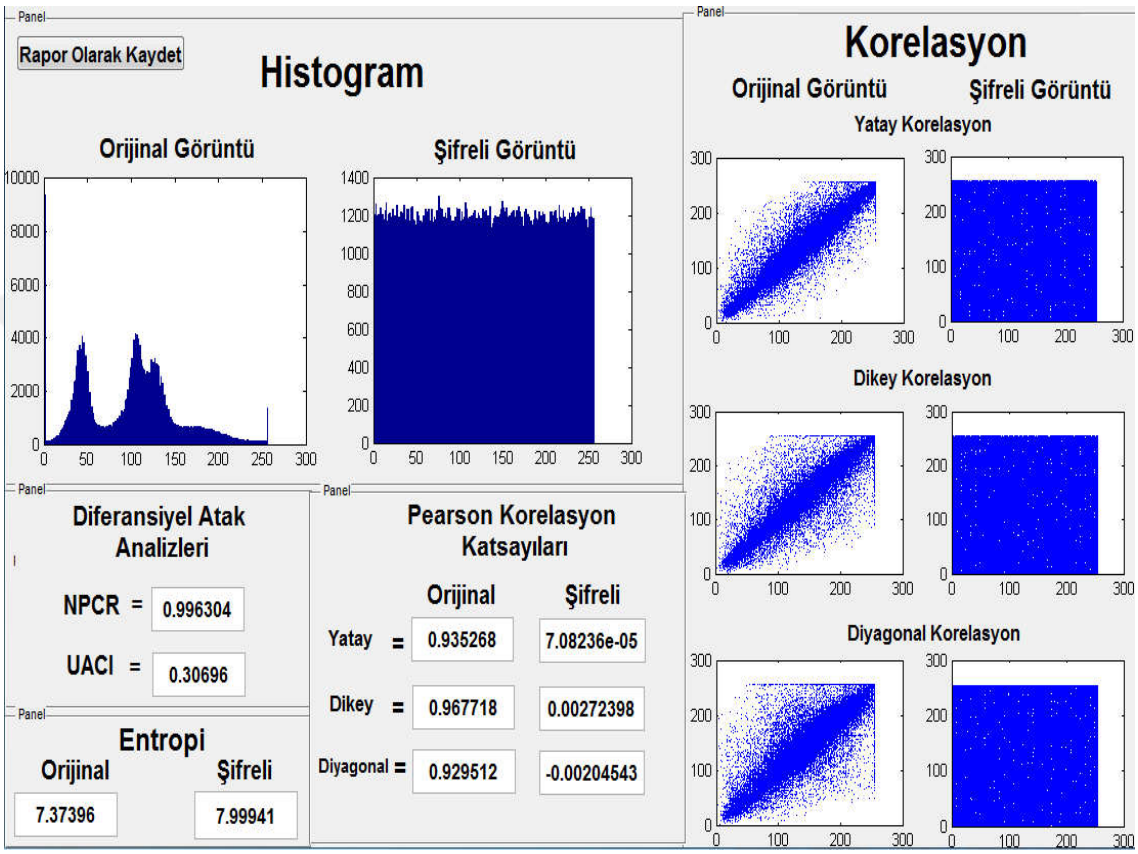
İstatistiksel Testler	**P-değeri (Y)**	**P-değeri (X)**	**Sonuç**
Frekans testi	0.8965	0.9968	Başarılı
Blok frekans testi	0.3889	0.1013	Başarılı
Akış testi	0.8243	0.5471	Başarılı
Bir Blok içerisinde En Uzun Birler Akış Testi	0.4219	0.9008	Başarılı
İkili matris derece testi	0.2445	0.0110	Başarılı
Ayrık Fourier dönüşüm testi	0.3773	0.7067	Başarılı
Örtüşmeyen şablon eşleştirme testi	0.4176	0.0773	Başarılı
Örtüşen şablon eşleştirme testi	0.8970	0.8649	Başarılı
Maurer'in "evrensel istatistik" testi	0.1658	0.2866	Başarılı
Doğrusal karmaşıklık testi	0.8497	0.4568	Başarılı
Seri testi-1	0.6249	0.1607	Başarılı
Seri testi-2	0.2244	0.0899	Başarılı
Yaklaşık entropi testi	0.7400	0.6918	Başarılı
Birikimli toplamlar testi	0.9645	0.6970	Başarılı
Rastgele gezinimler testi	0.1113	0.3686	Başarılı
Rastgele gezinimler değişken testi	0.0532	0.1105	Başarılı

Elde edilen sayı dizilerinin NIST 800-22 testi sonuçları Tablo 6.6'da gösterilmektedir. Test sonuçlarına göre rastgelelik testinden başarılı sonuçlar elde edildiği gözlemlenmiştir. Test işleminden başarılı sonuçlar alındıktan sonra şifreleme işlemi gerçekleştirilmiştir. Şekil 6.13'te S-kutusu & XOR Yöntemi ile gerçekleştirilen uygulamanın ilk kısmı olan şifreleme uygulaması verilmiştir.



Şekil 6.13. S-kutusu & XOR yöntemi ile video şifreleme işlemi

Şifreleme tamamlandıktan sonra "kaydet" butonu ile şifrelenen video, dosya ismi girilerek "*avi*" uzantılı dosya şeklinde kaydedilmektedir. "Analizler" butonu, videonun şifreleme işlemine tabi tutulmuş herhangi bir karesinin orijinal ile şifreli görüntüsünün analizini yapan bir panel çalıştırmaktadır. Bu analiz paneli Şekil 6.14'te verilmiştir.



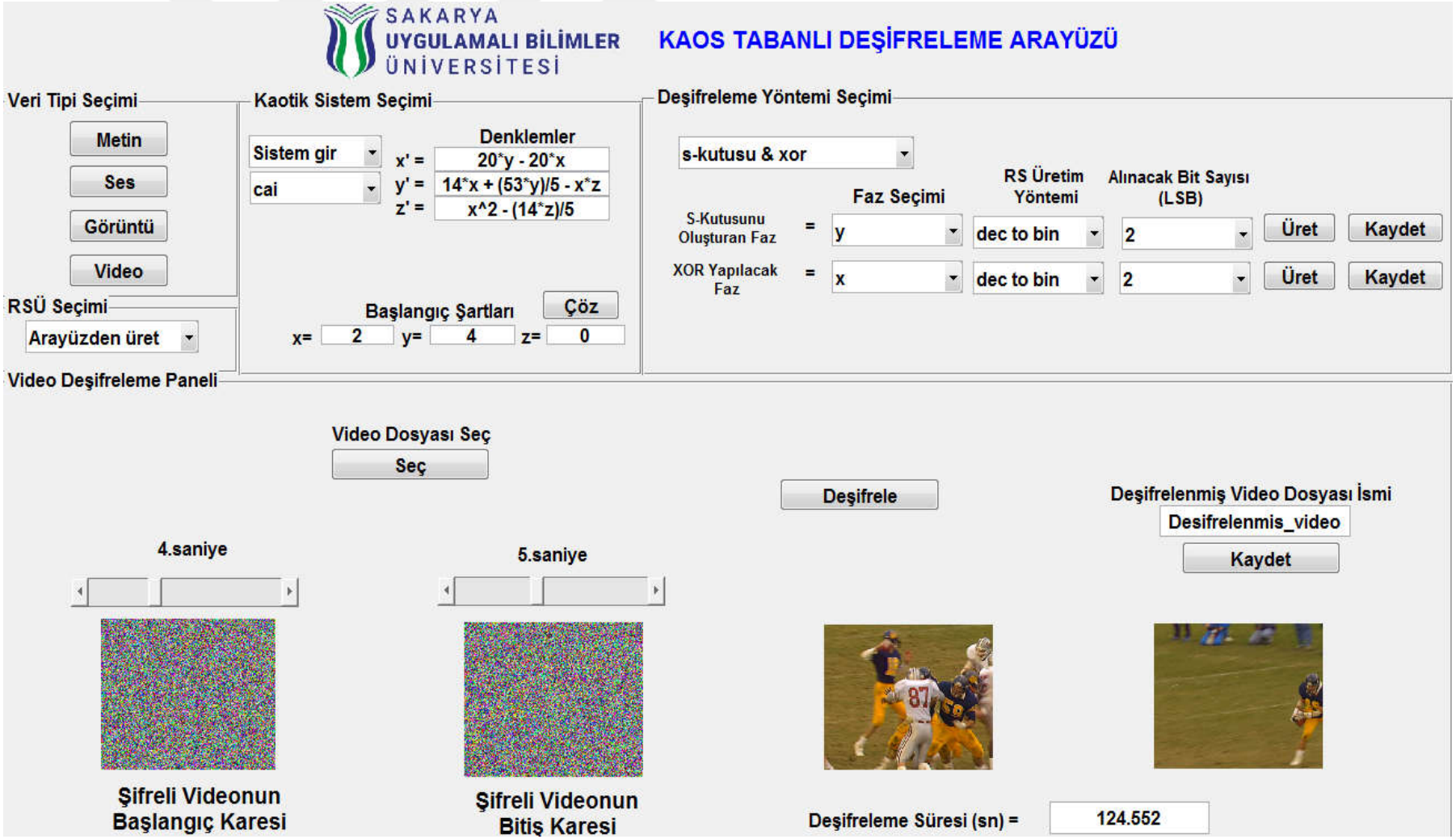
Şekil 6.14. S-kutusu & XOR yöntemi ile video şifreleme analiz sonuçları

Şekil 6.14'teki analiz panelinde orijinal ve şifreli video karesinin "R" kanalının analizleri gerçekleştirilmiştir. Histogram grafiklerinde, orijinal görüntünün histogramında bazı piksel değerleri daha fazla iken şifreli görüntünün histogramında değerler homojen bir dağılım sergilemiştir. Korelasyon analizlerinde ise yatay, dikey ve diyagonal korelasyon haritaları gösterilmektedir. Orijinal görüntünün korelasyon haritalarının hepsinde doğrusal bir grafik mevcutken, şifreli görüntünün tüm korelasyon haritalarında ise 0 – 255 değer kümesinin tümüne yayılan homojen bir grafik mevcuttur. Böylelikle 3 doğrultuda gerçekleştirilen orijinal ve şifreli korelasyon haritalarıyla komşu veri değerleri arasındaki güçlü bağların zayıflatıldığı görülmüştür. Yine 3 doğrultuda hesaplanan pearson korelasyon katsayı değerlerinin orijinal görüntü için 1'e çok yakın çıkması, şifreli

görüntü için 0’a çok yakın çıkması korelasyon haritalarının sonuçlarını destekler niteliktedir. Elde edilen NPCR ve UACI değerleri ile bu analizler için eşik değer olarak kabul edilen değerlerin üstünde olan sonuçlara ulaşılmıştır. Elde edilen entropi değeri bu analiz için ölçülebilecek en iyi değer olan 8’e çok yakın çıkmıştır.

Analiz sonuç değerlerine bakarak başarılı bir video şifreleme işlemi yapıldığı söylenebilir. Ayrıca panelde bulunan "Rapor Olarak Kaydet" butonu ile bu analizler bir rapor halinde Word dosyasına kaydedilebilmektedir.

Şekil 6.15’te video deşifreleme uygulaması gösterilmektedir. Şifreleme panelinde şifrelenen video, yeni bir kullanıcıya gönderildikten sonra kullanıcı deşifreleme panelinde doğru seçimleri (kaotik sistem, başlangıç şartları, rastgele sayı üreteci yöntemi, rastgele sayı üreteci yönteminde kullanılan faz, rastgele sayı üreteci yönteminde kullanılan hassasiyet bit değeri, şifreleme yöntemi) girdikten sonra şifrelenmiş video deşifre edilerek orijinal video elde edilir.



Şekil 6.15. S-kutusu & XOR yöntemi ile video deşifreleme işlemi

BÖLÜM 7. SONUÇ VE ÖNERİLER

Çoklu ortam dosyalarının saklanması ve iletişim uygulamalarında güvenli bir şekilde iletilebilmesi için şifreleme tekniklerinin kullanımı önemli bir yere sahiptir. Bu tez çalışmasında kriptoloji biliminde sıkça kullanılan kaotik sistemlerden ve yeni şifreleme algoritmalarından yararlanılarak, kaos tabanlı yeni bir çoklu ortam şifreleme aracının geliştirilmesi üzerinde çalışılmıştır.

Yazılım aracı tasarımının amaçları olarak önerilen kaos tabanlı şifreleme algoritmalarının daha rahat bir kullanım biçimi olabilmesi, şifreleme işlemlerinin sonucunda oluşan güvenlik analizlerinin tek bir panelde gözlemlenebilmesi ve şifreleme için kullanılan parametrelerin girdisinin daha kolay bir şekilde sağlanması gibi özellikler gösterilebilir.

Önerilen tüm şifreleme algoritmalarında çoklu ortam verileri anahtarlar aracılığıyla şifrelenir. Bu anahtarlar kaotik sistemlerin çıkış değerlerinden elde edilen rastgele sayılarla oluşturulur. Rastgele sayıların elde edilmesi için 3 adet rastgele sayı üreteci tasarım çalışması yapılmıştır.

Tasarlanan yazılım aracında referans kaotik sistemlerin bulunmasının dışında yazılım aracı, içerisine kullanıcı tarafından alternatif kaotik sistemlerin eklenip RK4 sayısal analiz yöntemine göre çözdürülmesine ve sonrasında da bu sistemlerin kaydedilmesine imkan sağlamaktadır.

Yazılım aracı, şifrelemede anahtar olarak kullanılacak rastgele sayıların nasıl seçilebileceği ile ilgili üç seçenek sunmaktadır. Bu seçimler; yazılım aracında bulunan mevcut kaotik sistemlerin değerlerinden üretilen rastgele sayılar, kullanıcı tarafından farklı kaotik sistemlerin yazılım aracına eklenmesiyle süregelen çözdürme işlemleri sonucunda üretilen rastgele sayılar ve direkt olarak rastgele sayıların bulunduğu *"txt"* dosya girişi ile gerçekleştirilir. Şifrelenen verinin türüne göre şifreleme sonrası oluşturulan güvenlik analizlerinin tasarlanan yazılım aracı üzerinden yapılması suretiyle her uygulama sonrasında şifreleme kalitesi hakkında bilgilere ulaşılır. Yapılan bu

güvenlik analizlerinin sonuçlarına kullanıcı tarafından daha kolay ulaşılabilmesi için yazılım aracına raporlama birimi entegrasyonu yapılmıştır.

Yapılan şifreleme uygulamalarında kaotik sistemlerin başlangıç şartlarına hassas duyarlılık göstermesinin rastgele sayı üretiminde ve devamında bu rastgele sayıların anahtar olarak kullanıldığı şifreleme uygulamalarının sonuçları için çok büyük bir etmen olduğu kanıtlanmıştır.

Yapılan uygulamalar neticisinde XOR, Tur sayılı XOR, S-kutusu & XOR ve Tur sayılı S-kutusu şifreleme yöntemlerinde veri kaybı olmaksızın şifreleme ve deşifreleme işlemleri gerçekleştirilmiştir. Uygulamalarda kullanılan kaotik sistemlerden elde edilen sayı dizilerinin rastgeleliği sağladığı, NIST 800-22 testinden çıkan sonuçlar ile birlikte yorumlanarak verilmiştir. Uygulamaların çıktı ve analizleri baz alınarak metin, görüntü, ses, video çoklu ortam verileri için şifreleme uygulamaları hakkında birtakım sonuçlara varılmıştır.

Metin dosyalarının şifrelenmesi sonucunda, şifrelenmiş metindeki karakter sayısının, orijinal metindeki karakter sayısına oranla daha fazla olduğu gözlemlenmiştir. Karakter çeşitliliğinin sayısının artması, algoritmaların yapısının her karakteri sadece belirli bir karaktere şifrelemediğini göstermektedir.

Görüntü dosyalarının şifrelenmesi sonucunda, şifrelenmiş görüntü dosyalarının güvenlilik kriterleri ile ilgili ipuçları veren histogram, korelasyon, entropi ve diferansiyal atak analizleri gerçekleştirilmiştir. Dört yöntem için de yapılan güvenlik analiz sonuçlarının literatürde bulunan bazı referans çalışmalarla karşılaştırılması yapılmış ve önerilen dört şifrleme yönteminin de görüntü şifreleme uygulamaları için başarılı sonuçlar verdiği gösterilmiştir.

Ses dosyalarının şifrelenmesi sonucunda, histogram, korelasyon ve PSNR güvenlik analizleri gerçekleştirilmiştir. Yazılım aracının sağlamış olduğu bazı işitsel bildirimler ile birlikte analiz çıktılarının değerlendirilmesi sonucunda önerilen yöntemlerin literatürde bulunan ses şifreleme yöntemlerine alternatif olabilecek yöntemler olduğu gözlemlenmiştir.

Yazılım aracı, video dosyası için 2 şifreleme seçeneği sunar. İlk olarak videonun tamamı şifrelenebilir veya video dosyası kısmi bir şifreleme ile önemli bilgilerin olduğu belirli bir kare grubu şifrelenebilir. Video analizleri gerçekleştirilirken videonun şifrelenen

zaman aralıklarından istenilen bir karenin görüntü şifreleme analizi gerçekleştirilebilir. Video dosyalarının şifrelenmesi sonucunda, görüntü dosylarında olduğu gibi histogram, korelasyon, entropi ve diferansiyal atak güvenlik analizleri gerçekleştirilmiştir. Önerilen yöntemlerin, video içerisindeki görsel verilere uygulanması sonucunda başarılı sonuçlar verdiği yapılan bu analizlerle gösterilmiştir.

Tüm bu çalışmalardan sonra elde edilen sonuçlar doğrultusunda, geliştirilen yazılım aracının güvenli haberleşme çalışmalarında bir uygulama aracı olarak kullanılabileceği öngörülmüştür.

KAYNAKLAR

[1] Pehlivan, İ., 2007. *Yeni kaotik sistemler: Elektronik devre gerçeklemeleri, senkronizasyon ve güvenli haberleşme uygulamaları.* Doktora Tezi, Sakarya Üniversitesi.

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

[3] Tien-Yien, L., & Yorke, J. A. (1975). Period three implies chaos. *Am Math Monthly*, *82*, 985-992.

[4] Varan, M. (2009). *Kaotik simulasyon laboratuvarı uygulaması.* Yüksek Lisans Tezi, Sakarya Üniversitesi.

[5] Huang, Z., Dong, W., Duan, H., & Li, H. (2013). Similarity measure between patient traces for clinical pathway analysis: problem, method, and applications. *IEEE journal of biomedical and health informatics*, *18*(1), 4-14.

[6] Pomares, J., Perea, I., & Torres, F. (2013). Dynamic visual servoing with chaos control for redundant robots. *IEEE/ASME Transactions on Mechatronics*, *19*(2), 423-431.

[7] Vaidyanathan, S. (2015). Adaptive backstepping control of enzymes-substrates system with ferroelectric behaviour in brain waves. *International Journal of PharmTech Research*, *8*(2), 256-261.

[8] Kaddoum, G., & Gagnon, F. (2013). Lower bound on the bit error rate of a decode-and-forward relay network under chaos shift keying communication system. *IET Communications*, *8*(2), 227-232.

[9] Yang, J., Chen, Y., & Zhu, F. (2014). Singular reduced-order observer-based synchronization for uncertain chaotic systems subject to channel disturbance and chaos-based secure communication. *Applied Mathematics and Computation*, *229*, 227-238.

[10] Volos, C. K., Kyprianidis, I. M., & Stouboulos, I. N. (2013). Experimental investigation on coverage performance of a chaotic autonomous mobile robot. *Robotics and Autonomous Systems*, *61*(12), 1314-1322.

[11] Yau, H. T., & Shieh, C. S. (2008). Chaos synchronization using fuzzy logic controller. *Nonlinear analysis: Real world applications*, *9*(4), 1800-1810.

[12] Matouk, A. E. (2011). Chaos, feedback control and synchronization of a fractional-order modified Autonomous Van der Pol–Duffing circuit. *Communications in Nonlinear Science and Numerical Simulation*, *16*(2), 975-986.

[13] Yılmaz, R. (2010). *Kriptolojik uygulamalarda bazı istatistik testler.* Yüksek Lisans Tezi, Selçuk Üniversitesi.

[14] Bulut Büyükgöze, S. (2012). *Modern bir blok şifre tasarımı.* Yüksek Lisans Tezi, Trakya Üniversitesi.

[15] Pecora, L. M., & Carroll, T. L. (1990). Synchronization in chaotic systems. *Physical review letters*, *64*(8), 821.

[16] Cuomo, K. M., Oppenheim, A. V., & Strogatz, S. H. (1993). Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Transactions on circuits and systems II: Analog and digital signal processing*, *40*(10), 626-633.

[17] Matthews, R. (1989). On the derivation of a "chaotic" encryption algorithm. *Cryptologia*, *13*(1), 29-42.

[18] Wong, K. W., Kwok, B. S. H., & Law, W. S. (2008). A fast image encryption scheme based on chaotic standard map. *Physics Letters A*, *372*(15), 2645-2652.

[19] Wang, Y., Wong, K. W., Liao, X., Xiang, T., & Chen, G. (2009). A chaos-based image encryption algorithm with variable control parameters. *Chaos, Solitons & Fractals*, *41*(4), 1773-1783.

[20] Xiao, D., Liao, X., & Wei, P. (2009). Analysis and improvement of a chaos-based image encryption algorithm. *Chaos, Solitons & Fractals*, *40*(5), 2191-2199.

[21] Liu, H., & Wang, X. (2010). Color image encryption based on one-time keys and robust chaotic maps. *Computers & Mathematics with Applications*, *59*(10), 3320-3327.

[22] Liu, H., & Wang, X. (2013). Triple-image encryption scheme based on one-time key stream generated by chaos and plain images. *Journal of Systems and Software*, *86*(3), 826-834.

[23] Prusty, A. K., Pattanaik, A., & Mishra, S. (2013, December). An image encryption & decryption approach based on pixel shuffling using Arnold Cat Map & Henon Map. In *2013 International Conference on Advanced Computing and Communication Systems* (pp. 1-6). IEEE

[24] Alsafasfeh, Q. H., & Arfoa, A. A. (2011). Image encryption based on the general approach for multiple chaotic systems. *J. Signal and Information Processing*, *2*(3), 238-244.

[25] Fındık, O. (2004). *Şifrelemede kaotik sistemin kullanılması.* Yüksek Lisans Tezi, Selçuk Üniversitesi.

[26] Liu, H., Kadir, A., & Niu, Y. (2014). Chaos-based color image block encryption scheme using S-box. *AEU-international Journal of Electronics and Communications*, *68*(7), 676-686.

[27] Ahmad, M., Alam, B., & Farooq, O. (2014). Chaos based mixed keystream generation for voice data encryption. *arXiv preprint arXiv:1403.4782*.

[28] abd ulkareem Nasser, M., & Abduljaleel, I. Q. (2013). Speech encryption using chaotic map and blowfish algorithms. *Journal of Basrah Researches (Sciences)*, *39*(2A), 68-76.

[29] Akgül, A. (2015). *Yeni kaotik sistemler ile rastgele sayı üreteci tasarımı ve çoklu ortam verilerinin yüksek güvenlikli şifrelenmesi.* Doktora Tezi, Sakarya Üniversitesi.

[30] Udwadia, F. E., & Guttalu, R. S. (1989). Chaotic dynamics of a piecewise cubic map. *Physical Review A*, *40*(7), 4032.

[31] Vlad, A., Luca, A., Hodea, O., & Tataru, R. (2013). Generating chaotic secure sequences using tent map and a running-key approach. *relation*, *1*, 0.

[32] Vajargah, B. F., & Asghari, R. (2015). A pseudo random number generator based on chaotic henon map (CHCG). *International Journal of Mechatronics, Electrical and Computer Technology (IJMEC)*, *5*(15), 2026-37.

[33] Mishra, M., Routray, A. R., & Kumar, S. (2014). High security image steganography with modified Arnold cat map. *arXiv preprint arXiv:1408.3838*.

[34] Arslan, C. (2019). *Tamsayılı ve kesirli dereceden farklı kaotik sistemler ile rasgele sayı üreteçleri ve arayüz tasarımı.* Yüksek Lisans Tezi, Sakarya Uygulamalı Bilimler Üniversitesi.

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

[36] Vaidyanathan, S. (2015). Global chaos synchronization of the forced Van der Pol chaotic oscillators via adaptive control method. *International Journal of PharmTech Research*, *8*(6), 156-166.

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

[38] Özer, A. B. (2005). *Elektriksel sürücü sistemlerinde doğrusal olmayan olguların kaotik analizi ve yumuşak hesaplama yöntemleri ile denetimi.* Doktora Tezi, Fırat Üniversitesi.

[39] Gökyıldırım, A. (2016). *Zayıf sinyal tespit uygulamalarına yönelik yeni kaotik sistem geliştirme yaklaşımı.* Doktora Tezi, Sakarya Üniversitesi.

[40] Bolotin, Y., Tur, A., & Yanovsky, V. (2009). *Chaos: concepts, control and constructive use*. Springer.

[41] Önal, O. (2013). *Kaotik elektronik devre tasarımı gerçeklemesi ve bir haberleşme uygulaması.* Yüksek Lisans Tezi, Bilecik Şeyh Edebali Üniversitesi.

[42] Koyuncu, İ., Alçin, M., Tuna, M., Pehlivan, İ., Varan, M., & Vaidyanathan, S. (2019). Real-time high-speed 5-D hyperchaotic Lorenz system on FPGA. *International Journal of Computer Applications in Technology*, *61*(3), 152-165.

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

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

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

[46] Cai, G., & Tan, Z. (2007). Chaos synchronization of a new chaotic system via nonlinear control. *Journal of Uncertain systems*, *1*(3), 235-240.

[47] Sprott, J. C. (1994). Some simple chaotic flows. *Physical review E*, *50*(2), R647.

[48] Sundarapandian, V., & Pehlivan, I. (2012). Analysis, control, synchronization, and circuit design of a novel chaotic system. *Mathematical and Computer Modelling*, *55*(7-8), 1904-1915.

[49] Zhou, W., Xu, Y., Lu, H., & Pan, L. (2008). On dynamics analysis of a new chaotic attractor. *Physics Letters A*, *372*(36), 5773-5777.

[50] Lai, Q., Nestor, T., Kengne, J., & Zhao, X. W. (2018). Coexisting attractors and circuit implementation of a new 4D chaotic system with two equilibria. *Chaos, Solitons & Fractals*, *107*, 92-102.

[51] Hu, G. (2009). Generating hyperchaotic attractors with three positive Lyapunov exponents via state feedback control. *International Journal of Bifurcation and Chaos*, *19*(02), 651-660.

[52] Güvenoğlu, E. (2006). *Görüntü şifreleme algoritmaları ve performans analizleri.* Yüksek Lisans Tezi, Trakya Üniversitesi.

[53] Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell system technical journal*, *28*(4), 656-715.

[54] Sakallı, M. T. (2006). *Modern şifreleme yöntemlerinin gücünün incelenmesi.* Doktora Tezi, Trakya Üniversitesi.

[55] Ertürkler, M. (2007). *Sayısal filigranlar ile kripto imzalarının birlikte kullanılması ve çoklu ortam verisi üzerindeki uygulamaları.* Doktora Tezi, Fırat Üniversitesi.

[56] Yavuz N. (2006). *Kaotik ortamlarda güvenli veri transferi.* Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi.

[57] Günden, Ü. (2010). *Şifreleme algoritmalarının performans analizi.* Yüksek Lisan Tezi, Sakarya Üniversitesi.

[58] Özkaynak, F., Özer, A. B., & Yavuz, S. (2011). Kaos Tabanlı Yeni Bir Blok Şifreleme Algoritması. *IV. Ağ ve Bilgi Güvenliği Sempozyumu BİLDİRİLER KİTABI*, *108*.

[59] Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International journal of bifurcation and chaos*, *16*(08), 2129-2151.

[60] Yalcin, M. E., Suykens, J. A., & Vandewalle, J. (2004). True random bit generation from a double-scroll attractor. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *51*(7), 1395-1404.

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

[62] Petrie, C. S., & Connelly, J. A. (2000). A noise-based IC random number generator for applications in cryptography. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, *47*(5), 615-621.

[63] Erkek, E. (2015). *Akış şifreleme algoritmaları kullanılarak rastgele sayı üretilmesi ve FPGA ortamında gerçekleştirilmesi.* Yüksek Lisans Tezi, Fırat Üniversitesi.

[64] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., & Barker, E. (2001). *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. Booz-allen and hamilton inc mclean va.

[65] Demirkol, A. Ş. (2007). *Kaotik osilatör girişli ADC tabanlı rastgele sayı üreteci.* Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi.

[66] Gupta, A., Thawait, R., Patro, K. A. K., & Acharya, B. (2016). A novel image encryption based on bit-shuffled improved tent map. *International Journal of Control Theory and Applications*, *9*(34), 1-16.

[67] Yildiz, M. Z., Boyraz, O. F., Guleryuz, E., Akgul, A., & Hussain, I. (2019). A novel encryption method for dorsal hand vein images on a microcomputer. *IEEE Access*, *7*, 60850-60867.

[68] Fu, C., Chen, J. J., Zou, H., Meng, W. H., Zhan, Y. F., & Yu, Y. W. (2012). A chaos-based digital image encryption scheme with an improved diffusion strategy. *Optics express*, *20*(3), 2363-2378.

[69] 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.

[70] Güleryüz, H. İ. (2014). *Gri seviye görüntülerde kriptografik uygulamalar.* Yüksek Lisans Tezi, Fırat Üniversitesi.

[71] Yıldız, Y. (2012). *Sırörtme yöntemiyle video üzeri şifrelenmiş güvenli iletişim uygulaması.* Yüksek Lisan Tezi, Sakarya Üniversitesi.

[72] Zhu, Z. L., Zhang, W., Wong, K. W., & Yu, H. (2011). A chaos-based symmetric image encryption scheme using a bit-level permutation. *Information Sciences*, *181*(6), 1171-1186.

[73] Wang, Y., Wong, K. W., Liao, X., & Chen, G. (2011). A new chaos-based fast image encryption algorithm. *Applied soft computing*, *11*(1), 514-522.

[74] Seyedzadeh, S. M., & Mirzakuchaki, S. (2012). A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. *Signal processing*, *92*(5), 1202-1215.

[75] Wei, X., Guo, L., Zhang, Q., Zhang, J., & Lian, S. (2012). A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Journal of Systems and Software*, *85*(2), 290-299.

[76] Hussain, I., Shah, T., & Gondal, M. A. (2012). Image encryption algorithm based on PGL (2, GF (2 8)) S-boxes and TD-ERCS chaotic sequence. *Nonlinear Dynamics*, *70*(1), 181-187.

[77] Huang, C. K., Liao, C. W., Hsu, S. L., & Jeng, Y. C. (2013). Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system. *Telecommunication Systems*, *52*(2), 563-571.

[78] KM, S. K., & Hiremath, A. U. (2013). Image Encryption using Modified 4 out of 8 code and chaotic map. *International Journal of Computer Applications*, *975*, 8887.

ÖZGEÇMİŞ

Tankut KURT, 05.03.1993'de İstanbul'da doğdu. İlköğretim eğitimini İstanbul'da, lise eğitimini Tekirdağ'da tamamladı. 2011 yılında Tekirdağ Şarköy Anadolu Lisesi'nden mezun oldu. 2012 yılında başladığı Sakarya Üniversitesi Elektrik - Elektronik Mühendisliği bölümünü 2016 yılında bitirdi. 2017 yılında Sakarya Üniversitesi Elektrik - Elektronik Mühendisliği bölümünde yüksek lisans eğitimine başladı.